By Nicholas Blank

Don't Let the Pandemic Launch Your New Product For You

With an economy stalled by the pandemic, companies are keeping new products under wraps and waiting for a better time to launch. But the longer new product campaigns are delayed, the more vulnerable they become to having specs leaked to the public. A rigorous investigation can preempt these leaks.

Maintaining secrecy before product launches has always been a challenge, particularly for tech companies keen on glitzy events to unveil the latest gadgetry. Wildly expensive product launches in venues like the Worldwide Developers Conference at the Brooklyn Academy of Music and the South by Southwest festival in Austin were *de rigueur*. But debuts like these have always been at risk of being undermined: In 2010, an Apple software engineer accidentally left his yet-to-be-released iPhone 4 at a bar in Redwood City, California. A few weeks later, the phone was in the hands of a writer at the tech blog, *Gizmodo*, who—before the unveiling—published a story with the banner: *This is Apple's Next iPhone*.

In addition to absentminded engineers losing prototypes, leaks can happen through other avenues:

- fan-club websites, common in the tech and automobile industries, often employ aggressive techniques such as using informants to collect photos and information; and
- supply chain leaks by disgruntled employees or subcontractors with access to critical components, prototypes, and finished products.

The pandemic has compounded the problem. Corporate security teams now wrestle with cybersecurity threats posed by a work-from-home (or live-from-work) reality; bad actor employees have more time to probe security gaps while away from daily supervision; and employees worried about layoffs may justify stealing pre-release products as an "insurance policy" of sorts.

While leaks are sometimes sanctioned by the company to whet consumer appetites, those done by outsiders can be extremely damaging. In a worst-case scenario, a sophisticated counterfeiter or competitor might reverse-engineer knockoffs before the genuine products reach the market. For

example, luxury brands know that criminal syndicates in Southeast Asia can make copies based on digital photos mere hours after fashion models strut the catwalks. While informed consumers of luxury products won't buy these knockoffs, brands lose the cachet of exclusivity when cheap copies land on e-commerce sites well before fashionistas can splurge at designer shops.

Savvy investigators can identify the details of pre-launch product thefts using interviews, computer forensics, and reviews of security systems. Controlled purchases of leaked samples can also help to identify breach sources. Another critical step, given that many of the fakes appear on e-commerce sites, is tracking counterfeiters via social media mapping and dark web research. Savvy companies look to investigators for theft prevention measures, including due diligence, cybersecurity reviews, and intelligence-gathering to identify potential offenders.

Measures that should be considered when mitigating the risk of pre-launch theft include:

- **Background investigations.** Investigators can seek human resources files on flagged employees with access to labs, sample rooms, databases, and other repositories where designs and photographs can be found. These files may contain poor performance reviews, notes on personality conflicts with managers, and formal warnings for violations as well as documenting an employee's privilege level. One type of threat common in emerging markets is undisclosed family relationships among employees. In factories where workers have been recruited from the same small villages and a workforce may number in the thousands, divided loyalties and conflicts of interest may exist. Unsuspecting companies in this position could find their head of security colluding with a relative working in logistics management to steal a prototype and falsify inventory paperwork to cover their tracks.

- **Intelligence gathering.** Companies can better prepare for potential intellectual property theft if they are armed with intelligence about possible threats. Probes of online discussion boards and the dark web may identify parties interested in acquiring pre-release products or offers to reward anyone who provides photos or samples. Companies can then escalate intellectual property protection levels by locking down prototypes or stopping all subcontractor access to them.

- **Security reviews.** Reviews to identify vulnerabilities should be broad in scope and examine intellectual property protection from a number of perspectives, including physical and IT security. Existing security measures should be assessed. Installing an expensive video surveillance system, for example, is not effective if no one monitors the video and the data is not saved for future review. And while companies may be able to maintain high security standards at their wholly-owned operations, they may have far less control over security issues at joint-venture and subcontractor factories. Accordingly, companies should require audit clauses in subcontractor contracts so security reviews and investigations can be conducted directly at subcontractor premises.

Despite the pandemic, companies should not surrender their ability to introduce new creations to the market at a time and place of their own choosing. An investment in intellectual property security background investigations, intelligence gathering, and the ability to activate a rapid-response investigation in the event of a leak can go a long way towards keeping the decision to launch a new product squarely in the hands of its owner.

About our firm

Nardello & Co. is a global investigations firm whose experienced professionals handle a broad range of issues including due diligence, anti-corruption & fraud investigations, civil and white collar criminal litigation and arbitration support, asset tracing, activist defense, political risk and strategic intelligence, digital investigations and cyber defense, monitorships and independent investigations, and compliance.

Our clients include the world's leading law firms and financial institutions, Fortune 500 and FTSE 100 companies, high-net-worth individuals and family offices, governments, NGOs, sports organizations, and academic institutions.

With offices in New York, London, Washington DC, Hong Kong, Tokyo, Milan, and Dubai, Nardello & Co. maintains a professional staff that includes former US federal prosecutors, US and international lawyers, former law enforcement personnel and intelligence operatives, licensed investigators, research analysts, former journalists, financial crime specialists, forensic accountants, and computer forensic experts.

Contact

Nicholas Blank
Managing Director
+852 3628 3950
nblank@nardelloandco.com

Nardello & Co.
WE FIND OUT