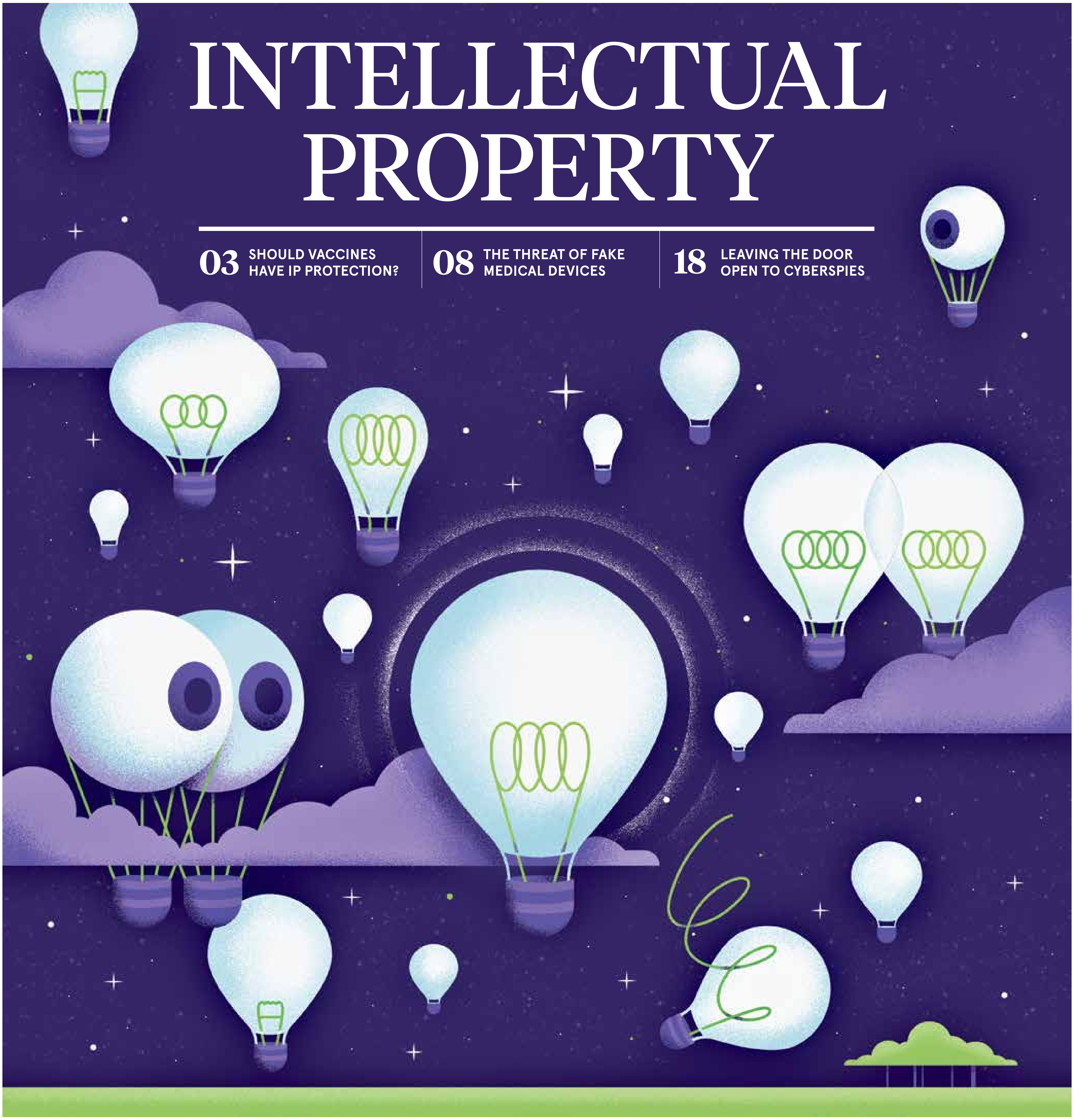
INDEPENDENT PUBLICATION BY RACONTEUR RACONTEUR.NET #0712 27/01/2021

INTELLECTUAL PROPERTY



Liyao Xie/Getty Images

CYBERESPIONAGE

Leaving the door open for cyberspies

COVID has left companies particularly vulnerable to cyberthreats, meaning adequate training for staff has never been more important

Marina Gerner

Cyberespionage conjures up nightmare scenarios for private and public organisations alike. While its true extent is hard to calculate as intellectual property (IP) cybertheft has largely remained in the shadows, with those affected preferring not to report losses publicly, its devastating impact is undeniable.

A former head of the National Security Administration has described cyberespionage as "the greatest transfer of wealth in history". According to the *CNBC Global CFO Council Survey*, one in five US-based companies said Chinese companies stole their intellectual property in 2018, an ongoing issue that has been at the heart of trade tensions between China and America.

Covid and a new risk environment for cyber threats

At the end of last year, the European Court of Auditors (ECA) warned that the coronavirus pandemic is likely to exacerbate cyber threats because many businesses and public services have moved from physical offices to remote working.

"The COVID-19 crisis has been testing the economic and social fabric of our societies. Given our dependence on information technology, a 'cyber crisis' could well turn out to be the next pandemic," says Klaus-Heiner Lehne, president of the ECA.

It is not only businesses, but governments and public institutions, that are at risk. At the end of last year, London local authority Hackney Council was hit by a cyberattack. Elsewhere, documents and data related to the Pfizer-BioNTech coronavirus vaccine have been stolen in a cyberattack on the European Medicines Agency in Amsterdam.

Since the outbreak of the pandemic, China and Russia-backed hackers have been accused of targeting research institutions. But as perpetrators of cybertheft evolve their techniques, so do companies when it comes to protecting their data.

Changing the playing field

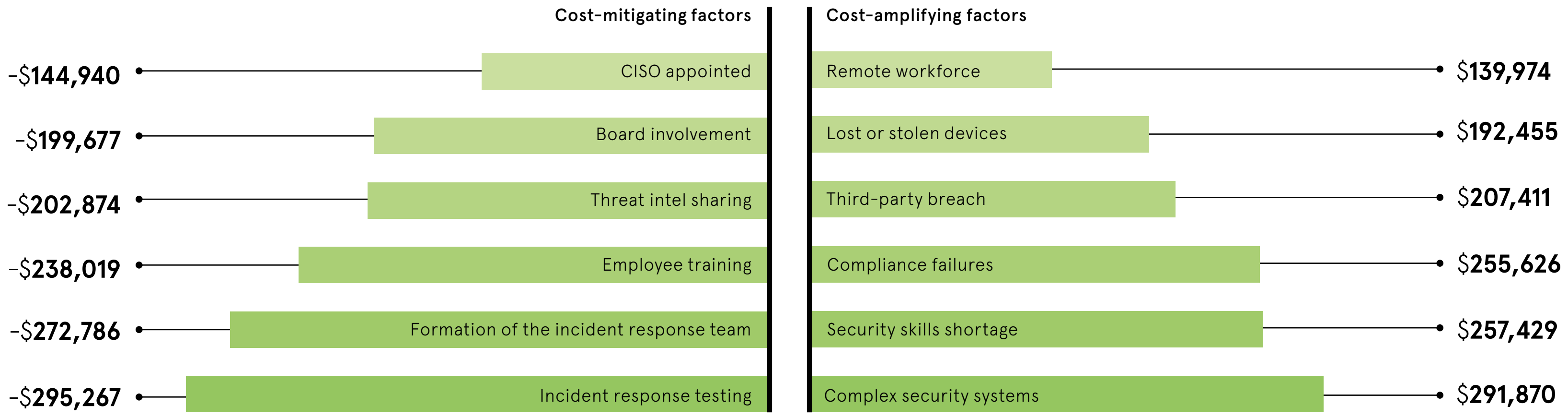
James Pooley, member of the Center for Intellectual Property Understanding and former deputy director general of the World Intellectual Property Organization, understands the full seriousness of cyberespionage.

Pooley agrees that COVID has created a riskier environment because employees are away from their usual offices. But the problem is not entirely current, he notes, explaining that a new risk environment emerged in the last 15 to 20 years, as we moved into an information-based economy, where the asset base shifted from tangibles to intangibles.

WHY PEOPLE ARE KEY TO CYBERTHREAT PROTECTION

IBM Security 2020

12 of the top factors that can boost or lessen the total cost of a data breach *(change in US$)*



In addition, "the imperatives for sharing information and trusting other people went up like crazy because of globalisation", he says. Supply chains have become longer and more complex, as companies shifted to vendors abroad and therefore have to manage their operations at a distance.

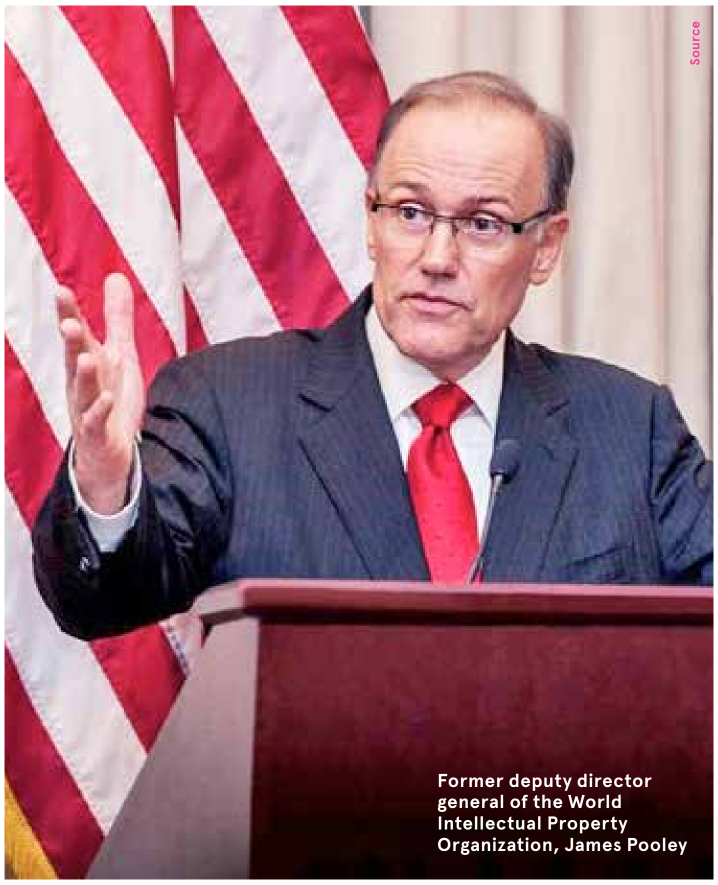
During the early-1970s, "all that a company needed to do to protect its information assets was to guard the photocopier and watch who went in and out the front door, because there were no networks, no internet and records were stored on paper", says Pooley. But, over the last decades, digitalisation coupled with globalisation has changed the playing field. Some of the most valuable assets have become intangible, opening up a whole new world to hackers.

So how does sensitive data end up in the wrong hands? Pooley argues that swathes of valuable information is lost because of employee inadvertence. In rough numbers, he says, "some 80 to 85 per cent of information loss occurs through employees, as opposed to hackers worming their way in from outside". While organisations can spend effort and money on secure IT infrastructure, they neglect employee behaviour at their peril.

The need to train employees to protect company IP

"I see it over and over again," says Pooley. "I get hired as an expert to critique the protection systems for companies in litigation over trade secrets, because they have to prove they took reasonable steps to prevent the things from happening." What he sees is companies neglect to train their employees on how to identify and handle confidential data.

Meanwhile, hackers look for the weakest link in a company's information chain, for instance when employees use the public wifi of a restaurant near their office for work purposes. He mentions the 2014 hack of Target, when the company's heating and air



Source

Former deputy director general of the World Intellectual Property Organization, James Pooley

> 80 to 85 per cent of information loss occurs through employees, as opposed to hackers worming their way in

conditioning contractor was used as an entry point by hackers, who exploited the vendor's weaker system to gain access to the Target system.

"It's just astonishing to me that more companies don't pay better attention to these issues, but there we are," says Pooley. "Maybe I'm a Cassandra, but remember, Cassandra was right."

How can companies train their employees to be more vigilant? "Preventing bad behaviour is usually about awareness, because people want to do the right thing and they want their jobs to be preserved," he says.

When Pooley advises companies, he begins with a high-level strategic examination of what the company's most important information assets are, what risks or vulnerabilities they face and what mechanisms there are to reduce these risks.

"Being really attentive to where the risk points are will alert you to pay special attention to areas that are likely to be used as points of entry," he says. Companies need to set up policies and procedures to ensure their IP is protected and training employees is a big part of that.

"I worked with one company that built a consumer product primarily manufactured in China, so there were obvious leakage risks connected to that." As they went through the process of developing a comprehensive system to protect their IP, Pooley asked for all the senior managers of the company to get together in one room to discuss the matter. Even though this was not easy to arrange, he insisted.

Overcoming silos to reduce IP vulnerabilities

Once all senior managers came together, including the supply chain managers who talked about issues they experienced directly, sharing information triggered insights for managers across the board.

"'Wait a minute, I don't think I've ever really looked at the non-disclosure agreement that we have with company x and when it expires.' All of a sudden, they're seeing vulnerabilities, where they hadn't really thought about them before," says Pooley. "No one expected the specialty arm of the organisation that dealt with all these companies in China would have something to say to the other business units, but vulnerabilities can overlap."

Are silos and inefficient communication partly to blame for companies' vulnerability when it comes to countering cyberthreats? Pooley argues organisations need to confront the fact that separate units within their business may have set up unnecessary walls. In reality, information flows and risks are usually shared across the business.

Part of the solution could be found through automation, he says, because automation includes behavioural analytics and insight tools that help companies monitor what exactly it is employees do on their platforms. However, using these tools always has to be balanced with individuals' expectations of privacy.

Pooley concludes: "The message that I often give is cyberespionage is scary and ugly, and we need to do everything we can to prevent it and deal with it. But if we're not managing our employees in a smart way, it's almost like we've left a couple of doors open." ●