November 16, 2016

Intellectual property breaches often carry hidden business costs

Cyber thefts can chip away at a company's reputation and bottom line for years

INFOGRAPHIC BY RODIKA TOLLEFSON, THIRDCERTAINTY

Père Francois Xavier d'Entrecolles, a Jesuit priest, traveled to China in 1712 and sent home letters revealing secrets of how Chinese craftsman produced beautifully delicate porcelain goods.

Clearly, industrial spying is as old as competitive commerce. Now the digital age has made it much easier to steal intellectual property. Yet data breaches related to IP theft rarely make news headlines.

That's surprising, considering that the loss to the U.S.

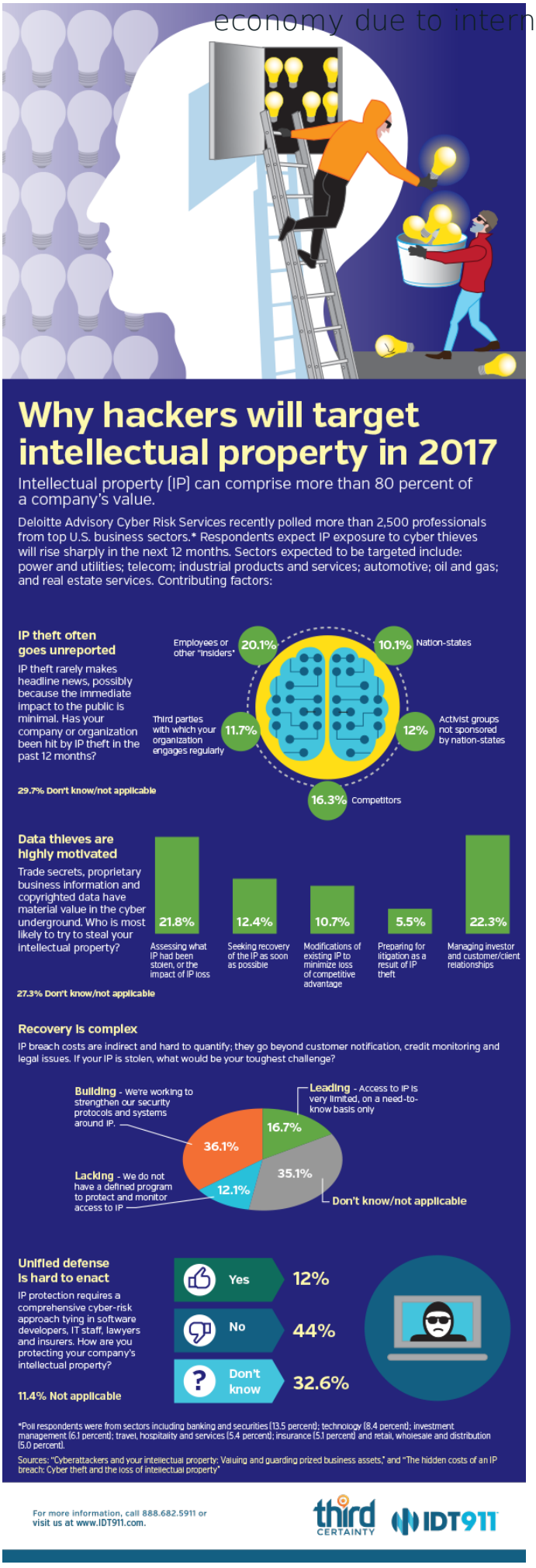
economy due to international intellectual property theft is estimated at $300 billion per year — and cyber theft increasingly is becoming the method of choice.

Related podcast: *Why network defense has become a core business concern*

Intellectual property is valuable to organizations because it creates a competitive differentiation in the marketplace, says Don Fancher, principal at Deloitte Advisory and global leader for Deloitte Forensics & Investigations.

"So obviously alerting the marketplace of the fact that there's been a theft of IP would not be in the best interest of the corporation," he says.

In a recent Deloitte poll of 3,000 professionals across multiple industries, managing investor, client and customer relationships was cited as the main challenge related to IP theft. Of 2,757 respondents to the question, 22.3 percent named that as the top challenge, followed by assessment of what IP has been stolen and the impact of the theft (21.8 percent).



Don Fancher, Deloitte

Fancher says the challenge of defining the extent of the breach may be another reason

why IP data breaches remain under the public's radar.

Advisory principal and Deloitte Forensics & Investigations global leader

"Often it's very difficult to fully understand what data may have been stolen," he says.

Perhaps the most surprising finding from the Deloitte poll was that 20 percent of the respondents pointed at employees and other insiders as the most likely to attempt IP theft. While insider threats, in general, have been a growing issue in cybersecurity, oftentimes those insiders are acting unwittingly or carelessly rather than maliciously.

"It's very easy to pick a villain and say it's some guy in a basement somewhere probing these networks. In fact, that's not always the case," says Scott Petry, CEO of Authentic8, a virtual browser solution provider.

Don't underestimate insider risk

Petry says organizations don't treat inside and outside risk equally, often putting a disproportionate amount of effort into protecting from outside actors.

Scott Petry, Authentic8 CEO

"It's crazy because we think about cybersecurity in the context of putting a bigger wall around the organization in order to keep the bad guys out," he says.

In an earlier report looking at the hidden impacts on businesses from cyber attacks, Deloitte identified loss of intellectual property as one of 14 cyber attack factors—and one of seven factors that stay beneath the surface because of hidden or less visible costs.

Related infographic: *The hidden costs of data breaches*

While assigning value to these kinds of intangible losses is difficult, awareness among organizations seems to be growing. Deloitte's poll showed that 17 percent of organizations had a strong focus on securing their intellectual property, and another 36 percent were working on improving their protocols. Additionally, 58 percent of

respondents believed the number of IP cyber theft incidents will go up in the next year.

Adnan Amjad, cyber threat risk management leader for Deloitte Advisory Cyber Risk Services, says that a few years ago, those numbers would have been much lower.

IP theft more often on radar

"There's a lot more recognition that these things happen," says Amjad, who also is a partner at Deloitte & Touche LLP. "I think there's an increasing awareness that IP theft is as big of, if not a bigger, challenge (than PII theft)."

Another area of increased awareness, he says, is that this is not simply a technology problem. More organizations are realizing that investing in technology is not enough, and they need to enable the processes around that technology.

Adnan Amjad, Deloitte Advisory Cyber Risk Services cyber threat risk management practice leader

"Technology is an enabler, but this is a business issue," Amjad says.

The first recommendation he makes to clients, he adds, is to determine what needs to be protected because "it's hard to protect everything effectively."

"Figure out what's really important from a business perspective and work with different stakeholders across the enterprise," Amjad says.

Petry believes the new iteration of cybersecurity threats—targeted, backdoor attacks rather than "front-door, bulk attacks" to steal credentials—means the owner of intellectual property is not the only one who should be concerned about protecting it. As companies outsource everything from legal and payroll to billing services, the outside vendors are just as much of a target.

"If people are actively trying to extract intellectual property, law firms (and other consultants or contractors) can be the weak link in the chain," he says.

Because organizations are so interconnected with their suppliers and vendors, Amjad expects to see more efforts to address insider threat through programs such as behavior analytics. These kinds of requirements already are coming down to contractors doing work for the federal government.

"Eventually, more and more organizations will require their contractors and suppliers to have some sort of analytics for their employee base," he says. "We see it already happening, especially in industries that are significantly regulated."