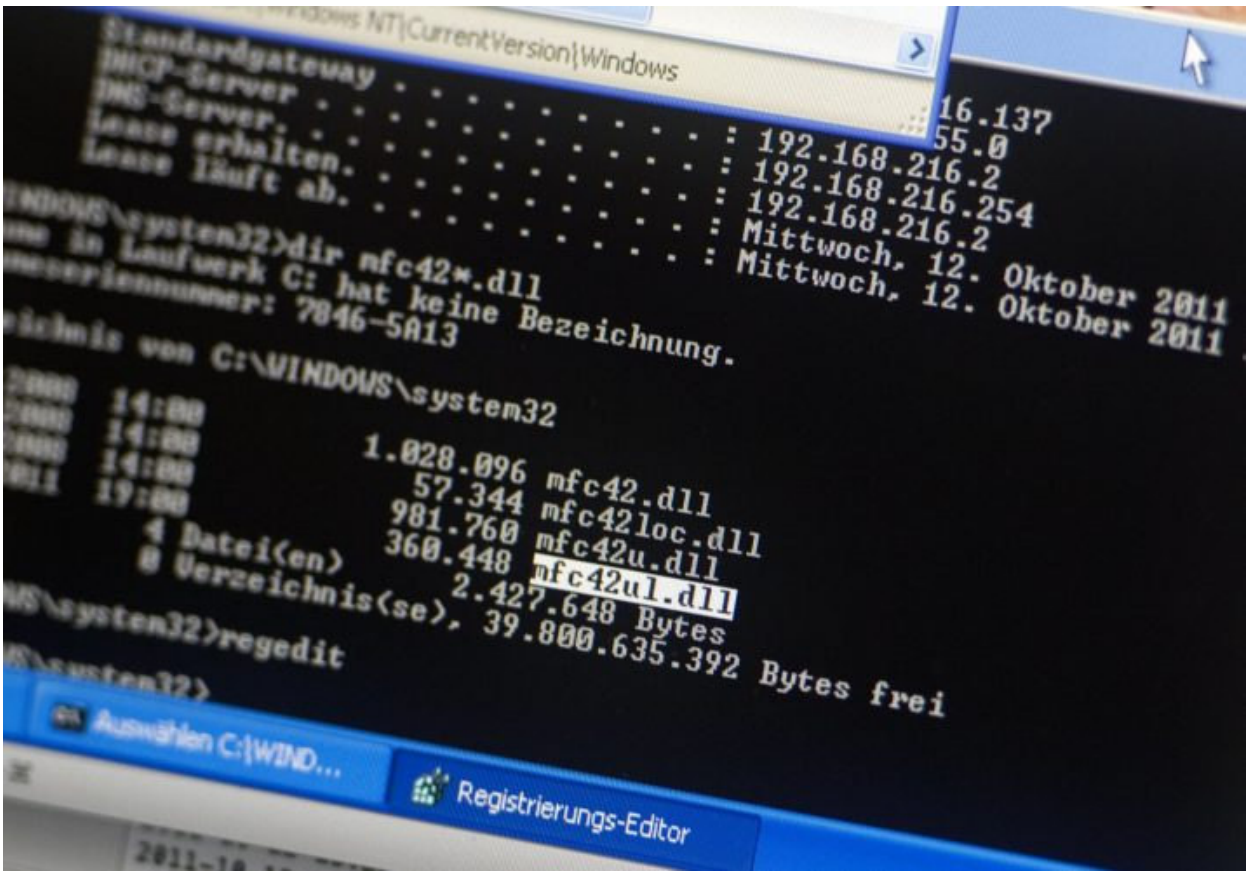
POLITICO



Odd Andersen/AFP via Getty Images

OPINION

Europe needs to build up its cyber defenses

Cyber insurance is the best tool for limiting cyber risk without giving up our economic competitiveness.

By **TIM STUCHTEY AND TYSON BARKER** | 2/23/17, 5:22 PM CET | Updated 3/2/17, 4:17 AM CET

Evidence of Russian cyber meddling in American presidential elections has reinforced one of the paradoxes of connectivity: The more digitally advanced we become, the more vulnerable we are. Cyber risks from pin-prick data theft to a full-scale "Cyber Lehman" pose an enormous threat to Europe and yet, for all the hype, we have not sufficiently built up our resilience.

Technology, regulation and military preparedness are all important puzzle pieces, but governments — and even members of industry, academics, hackers — cannot keep pace with the threat. There are many approaches to handling this issue. Among the most promising is something known as cyber insurance.

Two countries have typically dominated the field. American demand for cyber insurance has exploded as a tool for tackling cyber risk, driven largely by data laws in states like California, a string of high-profile incidents, and a litigious culture including the potential for class action lawsuits. Premiums in the U.S. currently top $3 billion and

are expected to rise precipitously in the next four years.

The U.K., meanwhile, is the main supplier — a kind of Saudi Arabia of cyber insurance accounting for between 20 percent to 25 percent of global market share. But the rest of Europe is largely out of the game. Attempts to mitigate cyber risk — on critical infrastructure, for example — are still limited to drafting regulatory protocols and voluntary standards.

Europe now faces the same type of high-profile cyber attacks suffered by the U.S. In recent months, we have witnessed successful attacks on a German steel mill and Ukrainian power plant; a major incident that knocked out the internet for almost 1 million German households; and mounting nervousness over Russia-sponsored hack-and-leak operations in the run-up to the Dutch, French and German elections.

> Cyber insurance could be a way to externalize digital risk and encourage more rapid digital transformation.

Europe has made digital transformation a core component of its plans for future competitiveness. But that goal will remain out of reach until business owners receive assurances that they are protected from digital risk. In Germany, for example, anxiety over potential cyber attacks means the adoption of digital services such as cloud computing is still spotty.

Under these circumstances, cyber insurance could be a way to externalize digital risk and encourage more rapid digital transformation.

* * *

Two mammoth new laws — one on data protection, the other on network security — are set to transform how Europe approaches cyber security. Together, these twin pieces of digital legislation will create new avenues for legal action and harsh financial penalties for companies that do not adequately address cyber risk and tighten up their digital protection game.

But right now insurers — like governments and businesses themselves — do not fully understand where the risk exposure lies. Many governments, including the U.S. and some EU member countries, can force companies to share information with national security agencies. The question becomes: How can this information be properly shared to help price risk in an accurate way? If mismanaged, sensitive information risks creating collateral damage to reputation and exposing company or governmental vulnerabilities.

Cyber risk can't be quantified in isolation. When assessing vulnerabilities, IT operators, insurers and policymakers need to think in terms of "too integrated" rather than "too big." Digitalization, like finance, is predicated on trust. And like finance, it enables other sectors to work productively.

A "Cyber Lehman" in particular — causing a cascade of failures across the internet, with potentially devastating effects for the financial sector and the economy — could max out insurance policies covering cyber risk. Policymakers will have to ensure private insurers are not scared out of the market and acknowledge that there are situations in which governments should step in as a reinsurer of last resort — as the U.S. did with terrorism insurance after 9/11. By providing a reinsurance backstop in limited cases, governments can encourage more insurance providers to enter the market and offer serious options beyond simple data breach coverage.

> Cyber attacks are among the top geopolitical risks of 2017.

Cyber insurers can support government cybersecurity efforts too. They can complement regulators by incentivizing companies to adopt standards and norms, train staff and embrace new cybersecurity technology. These could take the form of lower premiums and alliances between Silicon Valley and insurance providers that make state-of-the-art protections more rapidly deployable.

In some cases, particularly for networked devices like appliances, self-driving cars and even some industrial control systems, it could also mean wholesale liability transfer from consumers to the tech companies that manufacture these products.

Cyber attacks are among the top geopolitical risks of 2017. Europe has made strides to tackle this threat with new laws, regulations, military thinking and even behavioral norms. But without adding cyber insurance to its arsenal, Europe's economy and future resilience remain exposed.

Tim Stuchtey is the executive director of the Brandenburg Institute for Society and Security (BIGS), a civil security think tank based in Potsdam, Germany. Tyson Barker is a senior research fellow at BIGS. He was previously an official at the U.S. State Department.