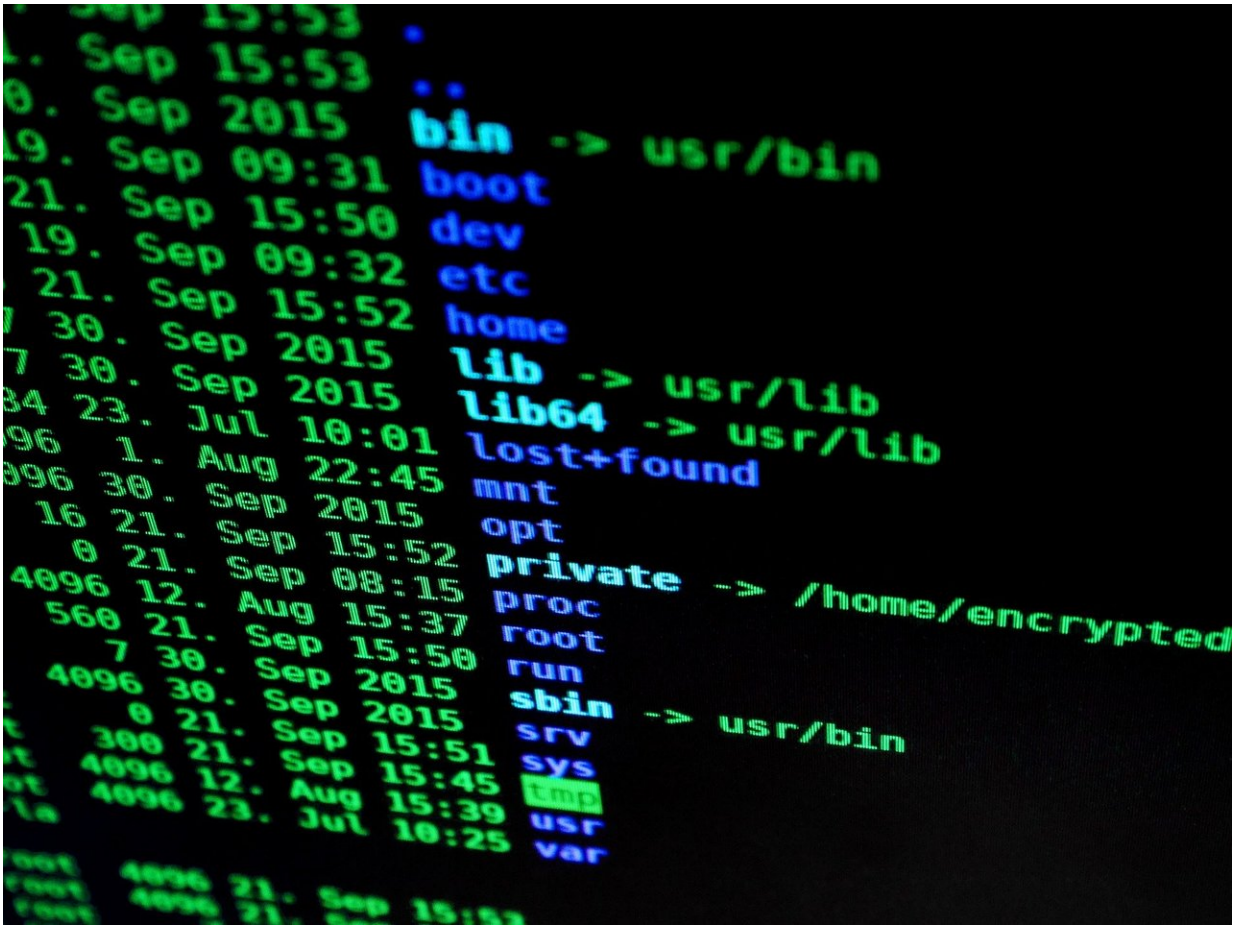
Cyberattacks and the economy: Assessing the damage

February 21 2020



Credit: CC0 Public Domain

When White House officials needed an expert to examine the economic

impact of cybersecurity threats, they called on Anna Scherbina.

Scherbina is an associate professor of finance at Brandeis International Business School. From 2017 to 2019, she served as a senior economist on the Council of Economic Advisers, the executive agency responsible for providing the president of the United States with objective advice on economic policy.

In this role, Scherbina literally wrote the chapter on cybersecurity in the 2018 Economic Report of the President. She drew particular attention to data breaches and concluded with her colleagues that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016, or upwards of 0.58 percent of gross domestic product.

"Companies collect a lot of data and innovate, but they don't always protect their data or intellectual property sufficiently well," said Scherbina. "Every year, the FBI is keeping tabs on thousands of security breaches."

Scherbina's work on the council covered a wide range of important and emerging topics—including international finance, FinTech and artificial intelligence. She also contributed to the chapter about AI in the council's 2019 report.

During a recent interview, Scherbina reflected on her work for the White House and why she thinks Brandeis is an exciting place to teach.

What are the consequences of data breaches and hacking?

I researched the impact of malicious cyber activity, no matter where it came from—cybercriminals, foreign hackers, other nation-states.

Foreign hackers are the most difficult adversary to deal with. I assessed the impact on the U.S. corporate sector and found that any given hack can reverberate throughout the economy, way beyond the company that was attacked. When one company is compromised, other businesses feel the impact too because everybody is so connected through different supply chain connections, and through similarities in the technology they use.

How do supply chains and technology amplify the damage?

Imagine if one company experiences a breach. It's now likely that other companies using similar technology or suppliers will have to investigate whether they were breached at the same time. And now you know there's some flaw—suddenly there's the possibility that everybody's exploiting it. In reality, other firms probably were breached too, but this information may never come out publicly.

Supply chains have turned out to be a cybersecurity vulnerability. Companies in a large firm's supply chain tend to be smaller with fewer resources. Generally speaking, the cyber capabilities of these companies are weaker than, say, a major retailer like Target. But remember the Target data breach? The hackers got in through Target's HVAC company. That's why it's very valuable to know who your suppliers are.

Where do you see artificial intelligence having a big impact?

Artificial intelligence is most useful when you have a lot of data to train it. So what industries will feel the biggest impact from AI? Maybe not finance because our time series is very short, meaning the data is not as good. The possibility of changing regulations also means we'll have

changing data patterns and that's a challenge for AI.

But healthcare is another matter because a disease is more or less always the same. This is an industry where you can really make advances. AI is not going to remove the need for doctors, but it could augment their work by being able to spot suspicious patterns that might be difficult to see with the naked eye.

I also see AI taking over tasks like report writing, so there's a potential impact on lawyers, financial analysts and others. But for something that requires a lot of creativity, especially in identifying the way patterns change, AI is far less effective.

How has Brandeis established itself as a leader in these areas?

We are at the forefront at Brandeis International Business School because we can be nimble. Here you can make decisions and adjust curricula very quickly. This is one of the advantages of teaching at a private university. In terms of education, being among the first business schools to move into some of these disciplines, like FinTech, we have this brand recognition that comes from the first-mover status. And we know that there are a lot of unfilled jobs, a lot of demand. So it's easier for our students to get hired, and through that, we're establishing enduring relationships with many up-and-coming companies.

Provided by Brandeis University