Cybersecurity expert Dmitri Alperovitch once said “In fact, I divide the entire set of Fortune Global 2000 firms into two categories: those that know they’ve been compromised and those that don’t yet know."

How much agreement is there about this thesis? Below is a collection of related quotes, plus one study that that bears on the question.

“I’ve since modified that phrase,” Alperovitch tells Fortune. “The first two companies still exist, but now **there’s a third type that’s able to successfully defend itself against intrusion.**” (source, 2019)

Alperovitch, 2020 [Protocol interview]

> On the private sector side, I have a view that we're in a fundamentally different place now than we were 10 years ago when everything seemed hopeless and you had no company that understood how to defend themselves against breaches from nation states and other sophisticated adversaries. **We certainly have the knowledge now for how to defend ourselves, and you don't hear about some of the largest companies having breaches.**

Richard Clarke, former White House counterterrorism and cybersecurity chief, and Robert Knake, senior fellow at the Council on Foreign Relations and a former director for cybersecurity policy at the National Security Council, 2019 [WSJ essay]

> Over the past 10 years, there has been encouraging news from the cyber realm: Many U.S. corporations have learned how to defend themselves from cyber criminals and even hackers deployed by hostile countries. The most quoted line at cybersecurity conferences has long been that there are only two kinds of companies: those that were hacked and knew it and those that were hacked and didn’t know. But now, **there is a third type of company: the “cyber-resilient” firm that suffers little or no damage when malicious hackers penetrate its network.**

The Fifth Domain [Book by Richard A. Clarke and Robert Knake] 2019

> In our analysis of public information on cybersecurity incidents, we found that less than a majority of the companies that make up the Fortune 500 had reported any significant cybersecurity incidents in the last decade. That means that the majority of the companies with the biggest bull’s-eyes on their backs have either succeeded in keeping the adversaries at bay or convinced their lawyers that whatever was taken did not merit a disclosure. For a small number of companies on that list, we have full faith that they have invested sufficiently and smartly to manage the risk and protect their most valuable assets. For others, we know for a fact that they have lost their crown jewels. (p. 48)
>
> Given this reality, any list of companies that have been hacked is going to be imperfect, and identifying companies that haven’t is even more difficult. **Yet we think there is**

solid evidence that some companies are effectively managing ongoing campaigns carried out by the most advanced and persistent actors. Battling those actors takes advanced skills and equal persistence on the part of defenders. It requires using threat intelligence and tracking actors inside networks. It requires building out a cooperative community to create a global detection grid of adversary behavior. (p. 49)

But many in the community will contend that if attackers are thwarted on one attack path, they will simply find another and eventually win. Inskeep thinks the data tells a different story. When Inskeep and other researchers at Booz Allen looked at that data, what they found suggests that many of the largest health insurance companies have done a pretty good job at keeping their customer data safe. While Anthem, the second-largest health insurer in the country, lost all of its subscriber data in 2015, some 78 million records, over the last five years the companies in the number one and number three positions in the market did not. Those companies, United Health and Aetna, respectively, lost a total of 12,000 records to cyber incidents. United Health, in fact, lost zero (though the company did report a small number of losses of files that had gone missing). Four of the remaining top ten health-care companies also reported zero losses to cyber theft. The three companies that round out the top ten reported a total of 37,000 lost records out of the 28 million records those companies hold. (p. 46)

Mike McConnell, Ex-NSA Director [speech at University of Minnesota], 2015

"The Chinese have penetrated every major corporation of any consequence in the United States and taken information," he said. "We've never, ever not found Chinese malware."

"I think his comment is reckless and misguided," said John Pirc, a former CIA cybersecurity researcher who launched his own cybersecurity software provider, Bricata. He said he's consulted at large companies after breaches and couldn't point the finger at China.

Robert Mueller, former FBI director, 2012 [speech at RSA]

For it is no longer a question of “if,” but “when” and “how often.”
I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

James Comey, former FBI director, 2014 [CBS' 60 Minutes interview]

There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.

Mikko Hypponen, chief research officer at F-Secure Oyj, 2016 [Business Insider interview]

> "How many of the Fortune 500 are hacked right now? The answer: 500," Hypponen said. "They all have security breaches, big or small. If you have a big enough infrastructure, you won't be able to secure all of it."

John Chambers, former Executive Chairman and CEO of Cisco, 2015 [World Economic Forum article]

> There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
>
> Major players in every industry were plagued by security breaches or incidents in 2014, though only the most high profile attacks made their way into the headlines. We found that 100% of business networks have traffic going to websites that host malware, and the number of cybersecurity incidents involving U.S. government agencies jumped 35% between 2010 and 2013. There is no indication that this is going to subside, and trends show that attacks continue to evolve in their sophistication and frequency. Because of this, it's no longer a question of if – but when – cybercriminals will get into our networks or data centers.

Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model, 2014 [report by FireEye and Mandiant]

> FireEye analyzed real-time data generated automatically by 1,614 appliances in proof-of-value (PoV) trials among 1,216 organizations across the globe from October 2013 to March 2014.
>
> Nearly all (97 percent) organizations had been breached, meaning at least one attacker had bypassed all layers of their defense-in depth architecture.
>
> 27% of all organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.
>
> The implication is clear: no corner of the world is remote enough to avoid falling into attackers' crosshairs, and current defenses are stopping virtually none of them.