Shareholder Demands More Tesla Accountability After Cybersecurity Close Call

Cybersecurity Expert and Tesla Shareholder Says Elon Should Be More Transparent to Shareholders About Cybersecurity Readiness After Attack

DENVER, CO, UNITED STATES, September 1, 2020 /EINPresswire.com/ -- "Elon Musk is a national treasure, and I thank him for immigrating and becoming a U.S. citizen," says Ray Hutchins, a Tesla shareholder and co-owner of two cybersecurity companies.

"I'm glad that Musk is competing in the Chinese market...I wish him well and hope that our two countries can learn how to compete while still treating each other with respect. But the hard reality is that the Chinese government has made it national policy to blatantly steal vast amounts of our intellectual property and to use those thefts against us economically, scientifically, and militarily. Other countries and criminals are doing the same thing. In light of these unfortunate facts, I urge all Tesla shareholders to demand more information about how Tesla's management is protecting our intellectual property and the value of our investments."

> All of us can still love Elon while demanding more cybersecurity transparency. Cybersecurity impacts valuation, so the subject should be front and center at the shareholder meeting on September 22nd."
>
> *Ray Hutchins*

Hutchins' comments were prompted by the recent, unsuccessful insider attack on Tesla as widely reported last week in the press. "I'm super grateful that the recent attack was thwarted and I offer thanks to the loyal Tesla employee and kudos to the FBI," Hutchins said. "But it was only luck that that guy didn't take the $1M and provide access into Tesla's IT infrastructure. I worry that other attackers are already silently operating within Tesla and doing God-knows-what. No way was this recent attack the only effort to break into Tesla."

Shareholders of all publicly traded companies must trust that management is doing its job with

respect to protecting company data, intellectual property, and valuation. But there is no shortage of evidence showing us how such trust is often misplaced. Cybersecurity breaches in 2020 include: Landry's Restaurants, Microsoft, MGM Resorts, Estee Lauder, Walgreens, Carnival Cruise Lines, T-Mobile, GE, Marriott International, Zoom, Facebook, Nintendo, GoDaddy, Twitter, Instagram, TikTok, YouTube and more.

"Considering the enormity of the business risk, I'd expect more real discussion of cybersecurity risk in Tesla's 10-K and also by Elon, who is always in the news," said Hutchins. "I don't want him or Tesla's management to reveal any tactical secrets, but more information about how they are devoting adequate attention and resources to this critical risk would be reassuring."

Hutchins was referring to previous statements by other CEOs about their cybersecurity efforts, such as JP Morgan Chase's CEO Jamie Dimon who said that his bank spends half a billion dollars a year on cybersecurity. And former Wells Fargo CEO John Stumpf who said that they were spending an “ocean” of money on cybersecurity and that this was the only expense where he asks if they are "spending enough."

Hutchins says that cybersecurity is now at the core of company valuations. "If a company cannot protect its IT infrastructure, data, and intellectual property from attack, then it is worth less than a company that can." He added, "Tesla has a very rich valuation which I believe is warranted...but only if it can protect its assets during this economic cyber war. I think all Tesla shareholders want the company to protect and grow the company's valuation."

It seems that Hutchins knows something about cybersecurity and company valuations. He was the first cybersecurity professional to approach the National Association of Certified Valuators and Analysts (NACVA.org) to formally request a change in the business valuation standard to formally include cybersecurity due diligence. As a result, that change is now underway.

Hutchins says that his companies are part of the DoD's effort to protect the nation's Defense Industrial Base (DIB) from cyber attack via its new Cybersecurity Maturity Model Certification (CMMC) program. After the General Service Administration (GSA) announced that they were going to follow DoD's lead and require CMMC certification before awarding GSA contracts, it is expected that all federal agencies (and then state governments) will ultimately do the same.

Hutchins' partner, Mitch Tanenbaum, a cybersecurity professional for over thirty years, says that publicly traded companies like Tesla should implement programs at least as good as the DoD CMMC program. "Our country is suffering huge intellectual property and financial losses right now. All publicly traded companies like Tesla should have already built or be building Level 5 CMMC-equivalent programs."

"I'll take that a step further," says Hutchins. "I think Elon should tell the public how SpaceX and his other privately-held companies and investments are protecting their intellectual property. SpaceX is already doing work for the DoD, and all of us have a stake in Elon's success, whether

we are investors or not."

"Tesla has a huge base of loyal shareholders who have a vested interest in this conversation," Hutchins says. "All of us can still love Elon, his visions, and execution while demanding more cybersecurity transparency. Cybersecurity impacts valuation, so the subject should be front and center at the shareholder meeting on September 22nd."

When asked why he was so alarmed now when the recent breach had been stopped, Hutchins said, "That breach is not the problem...only a symptom of the problem. Tesla has to stop all the breaches every time, the criminals only have to succeed once. Now is when we, as shareholders, must demand that Elon stays on point and protects our investments."

Hutchins and Tanenbaum are partners in CyberCecurity LLC and Turnkey Cybersecurity and Privacy Solutions LLC (TCPS) which is the leader in TURNKEY cybersecurity programs for smaller companies who have to comply with DoD CMMC, NIST Cybersecurity Framework and other requirements. TCPS is the only company to offer small to medium-sized companies this cost-effective option. TCPS has a full range of pre-engineered, turnkey, comprehensive cybersecurity and privacy programs for smaller companies. Their programs make cybersecurity easier, less brain-damaging, and less expensive and the programs include full cybersecurity support - because it cannot be done otherwise.

For more information, please contact:

Ray Hutchins
CyberCecurity LLC
+1 303-887-5864
email us here
