Hot Cyber ETFs Trade

By: TradeWins Publishing

Cyber Threat 2017: We Haven't Dodged this Bullet

"We haven't full dodged this bullet at all…"

Days after one of the most vicious cyber attacks crippled the world, that's what Ryan Kalember, senior vice of ProofPoint Inc. feared the most the day after.

"Until we're patched against the vulnerability itself," he notes, we're still in harms way.

No one is safe. In fact, not even you or the U.S. government.

Our own U.S. government has had a target on its head for years.

Yet it's not prepared at all.

"According to a recent federal edition of Thales Data Threat Report, 34% of federal respondents experienced a data breach in the last year and 65% experienced a data breach in the past. Almost all (96%) consider themselves 'vulnerable', with half (48%) stating they are 'very' or 'extremely' vulnerable," as reported by Axios.

Embarrassingly, a day after President Trump signed an executive order demanding broad review of cyber security at the federal level; the world was hit with a vicious Ransomware virus.

More than 200,000 companies in 150 countries wee hit, including the U.S., the UK, China, Germany, France and Russia. Thousands of computers were affected in China for example, shutting down gas stations, cash machines and universities. Hospitals in the UK were forced to close. Emergency rooms turned away patients.

Granted, a kill switch was flipped not long after. But the threat is still very real. In fact, there's a new attack happening right now. According to cyber security-company, Proofpoint Inc. (PFPT) the latest virus installs a program called Adylkuzz, which mines for crypto currencies on victims' computers. It's likely to impact older, unpatched versions of Windows, though.

But it highlights something very interesting.

We were never prepared. According to IBM, up to 68% of companies are not prepared for attacks, as of November 2016. Up to 75% of companies do not have a cyber security attack plan. Up to 74% say they faced threats because of human error. Up to 66% are not confident in their company's ability to recover from an attack.

Worse, Microsoft predicts that by 2020 data volumes online will be 50 times greater than what they are today with 111 billion lines of new software code produced each year, including billions of potential vulnerabilities that can be exploited.

We could go on. But you get the idea.

Unfortunately, those failures affect each one of us, too. Each time a trusted company screws up, most times, consumers are having their most private data exposed for the world to see. Credit cards, social security numbers, bank account information, even your child's information in the

hands of strangers.

Yet, we're nowhere near ready for the next attack.

But in every crisis, there is opportunity. In fact, smart investors have been flocking to cyber security ETFs, like the Pure Funds ISE Cyber Security ETF (HACK), which gives traders access to some of the hottest sector stocks, like FireEye (FEYE), Splunk (SPLK), Check Point (CHKP), Symantec Corporation (SYMC) and even Fortinet (FTNT).

The best part of an ETF – you can own more for less.

For instance, you can buy ten shares of FEYE, SPLK, CHKP, SYMC and FTNT for a total price of $2,570.25, or you can buy 10 shares of the HACK ETF for $290.72.

We'll leave the better choice up to you.

However, if you're an options trader on the cyber threat breakout, another interesting way to trade the fiasco has been with the September 2017 115 calls, which carry a delta of 0.5115. Others are simply buying PANW shares and holding, long-term.

PANW is the 800 lb. gorilla of the sector. After gapping down as badly as it did in early March 2017, it's become one of the cheapest ways to trade the cyber security issue. While it has pulled back in recent weeks, any further incidences of cyber attacks is sure to send it back up quick.

It's just something to think about as the cyber threat grows in an unprepared society.