Top Cybersecurity Breaches in 2018 Could Have Been Avoided, According to Cybersecurity Firm, VirtualArmour

January 15, 2019

CENTENNIAL, Colo., Jan. 15, 2019 (GLOBE NEWSWIRE) -- Several major cybersecurity breaches surfaced last year, from Google, Facebook and British Airways to T-Mobile, Uber and Marriott. Lapses in security exposed the personal data of hundreds of millions of individuals to unauthorized users. These were in addition to the countless number of other breaches around the world that went unreported.

Unfortunately, these events could have been avoided. “Last year’s major data security breaches could have been prevented with a properly implemented cybersecurity strategy and proactive management,” according to Andrew Douthwaite, chief technology officer at VirtualArmour International (OTCQB:VTLR, CSE:VAI, F:3V3), a fast-growing cybersecurity managed services provider based in Denver, Colorado.

Leading the growth of VirtualArmour over the last decade, Douthwaite knows a few things about Cybersecurity, and his company’s track record shows it. “While there were plenty of attempts, none of our enterprise clients were breached utilizing our services in 2018 – or ever, for that matter, since they became a client – and for good reason,” said Douthwaite. “We are the best at what we do.”

2018 taught us a lot about cybersecurity and the consequence of not having robust policies in place. Last October, Google announced it discovered a security bug in Google+ that allowed unauthorized access to private user data. This included a wealth of personal information, including full names, occupations, birth dates, email addresses, personal photographs, addresses, and relationship status.

This breach, which played out between 2015 and 2018, affected hundreds of thousands of users. If this was not bad enough, Google+ suffered a second major data breach only a few months later that affected another 52.5 million users. According to Douthwaite, these breaches could have been avoided if the security bug had been identified early and if a patch had been immediately created and deployed.

Such breaches can also be costly. Last year, Uber was forced to pay $148 million to the Federal Trade Commission after falsely claiming that they closely monitored internal access to customers' personal information. The FTC also found that Uber had not lived up to its promise to provide a reasonable level of cybersecurity to safeguard customer data. This settlement stems from two separate data breaches that occurred in 2015 and 2016.

These major security events highlight how opportunities for specialized service providers like VirtualArmour have grown in line with the increasing volume of cyber-attacks against businesses, non-profits and government institutions. This shift has not only led to increasing enterprise budgets being allocated to cyber protection, but also greater interest in investment opportunities in this high-growth sector.

According to Cybersecurity Ventures’ recent quarterly report, global cybersecurity spending is predicted to exceed $1 trillion cumulatively from 2018 to 2021. In 2004, the global cybersecurity market was worth $3.5 billion. In 2018, spending is expected to hit $120 billion.

Along with the increasing demand for cybersecurity solutions, many cybersecurity hardware and software stocks also realized strong gains in 2018. As the only publicly-traded pure-play cybersecurity managed services provider in North America, VirtualArmour is well positioned to capitalize on the industry growth opportunity.

VirtualArmour services a wide range of clients, which include Fortune 500 companies and several industry sectors in over 30 countries across five continents. Its customized solutions help businesses build, monitor, maintain and secure their networks, and it maintains 24/7 client monitoring with specialist teams located at its U.S. and UK-based security operation centers.

The company’s proprietary CloudCastr client platform provides clients with all-in-one dashboard with unparalleled access to real-time reporting on threat levels, breach prevention and overall network security.

“While the big breaches in 2018 are behind us, companies should brace for more sophisticated and devastating attacks in the new year,” said Douthwaite. “Cybercrime remains a seriously strong threat, and every business manager should be taking steps to ensure that their company does not become a successful target.”

Douthwaite delves more into these simple solutions and other major 2018 breaches in a recent article published on LinkedIn.com here.

For more information about what steps a company should take to safeguard sensitive information, contact VirtualArmour at (720) 644-0913 or email here. To learn more about VirtualArmour as a publicly-traded company, contact Ronald Both or Grant Stude at (949) 432-7566 or email here.

Source: VirtualArmour International Inc.