The Cybersecurity Implications of Brexit for Your Company

By Venkat Rajaji, Senior Vice President Marketing, Core Security

Some analysts view the U.K.'s vote to leave the European Union as the catalyst for economic turmoil – from roiling the U.K. real estate market to the slowdown in various vertical markets.

While many implications associated with Brexit are being discussed, it may take years to see the long-term impact. That said, we already are seeing the initial economic impact and slumping investor confidence resulting from this political decision. Companies noting this global market volatility may be tempted to cut costs as a proactive measure. This may be the appropriate thing to do in some circumstances. However, **it is critical to have a heightened sense of awareness around what Brexit means for your company's information security policies.** When evaluating the importance of information security, consider the following questions for your business:

1. How does this politically motivated decision impact our business, and specifically, the information security of our business?
2. Could we become more of a target as a result of this decision?

3. If we are more of a target, where are our exposures?
4. What should we be focusing on in terms of preventing and responding as quickly as possible to potential breaches?

The idea you may be more vulnerable as a result of a political decision, such as Brexit, is not new, but this does not make it any less real. Anytime there is opposition to a political action, businesses may be vulnerable to an attack, whether from a nation-state or otherwise.

While we don't necessarily understand the motivations behind adversaries, Brexit could be a motivator for bad actors. For example, in 2014, Sony produced a comedic movie with a political statement about Kim Jong-un, and North Korea backlashed by hacking their network and releasing private emails.

So what are the precautions your company should take given this landscape? Three critical information security policies can lessen impact of potential attacks on your business.

1. **Manage privileged accounts, aka the keys to the kingdom.** Privilege misuse was the second-most common cause of security incidents and the fourth-most frequent cause of breaches, according to the 2016 Verizon Data Breach Investigations Report (DBIR). Your business should continuously monitor privileged credentials to make sure they are not exposed.

2. **Manage user credentials and identities.** The same Verizon report also found 63 percent of data breaches are associated with the misuse of legitimate user credentials. Businesses in all industries need to manage the growing universe of identities, devices and data employees require to do their jobs.

3. **Understand your network vulnerabilities.** Businesses must efficiently identify and prioritize vulnerabilities for remediation. You need to constantly work in protection

mode to prevent attacks from penetrating your network.

4. **Conduct continuous penetration testing.** Businesses should implement penetration testing and certification reviews to continuously validate your users and your network. These are vital best practices for comprehensive security policies.

The bottom line during this time of economic and investor uncertainty following the Brexit decision is that businesses must have a heightened sense of awareness around their cybersecurity. Given the controversy surrounding Brexit, investors and executives are wise to consider the cybersecurity implications for their company and understand why information security is not an area for cost cutting measures.

If you are a target, you should be aware you're a target. Know that you cannot stop an attack on your network, but you can stop hackers from penetrating valuable data in your network. Your company needs to have policies in place to rapidly determine the root cause of a vulnerability and prioritize the correct mitigation action as quickly as possible.

About the Author: Venkat Rajaji is the Senior Vice President of Marketing and is responsible for business development and lead generation at Core Security. Venkat brings with him diverse expertise in marketing, product management, management consulting, finance, and presales. Before joining Core Security, Venkat was Vice President of Sales Operations and Customer Retention at Aptean. He also held product management and marketing roles with Infor and consulting roles with IBM and Accenture. Venkat received a Bachelor of Arts from the University of Texas-Austin, master's degree in Information Management from University of Maryland-College Park, and a Master of Business Administration from the Goizueta School of Business at Emory University.