Neustar Research Finds Global Attacks Like WannaCry and GoldenEye Directly Affect Enterprise' Cyber Protection Choices

Jul 19, 2017

NISC International Cyber Benchmarks Index™ launches as hundreds of EMEA security professionals contribute valuable data that can increase industry awareness and improve cyber-attack defense

Neustar, Inc. (NYSE:NSR), a trusted, neutral provider of real-time information services, today announced the results from a new survey of 290 security executives from across 11 EMEA countries. Sixty percent of respondents confirmed that the recent global attacks, such as WannaCry, had a direct effect on the way they protect their enterprises.

The findings are part of a broader survey, conducted by the Neustar International Security Council (NISC), which will be used to compile an ongoing Cyber Benchmarks Index™. Based on the personal opinions from hundreds of security professionals, including business managers, senior directors, CTOs and other professionals with a security remit and extensive cybersecurity industry experience, the Cyber Benchmarks Index enables NISC members and the wider cyber community to track changes and trends in the perception and attitudes of security professionals in relation to the threat landscape. The index is a genuine pan-EMEA view that will reveal valuable industry trends, such as which threats are currently of most concern, how the threat of attack by different vectors changes over time and perception of where threats originate.

"The majority of respondents indicating that recent global attacks have directly affected their protection choices shows that while awareness exists, it is clear that there's a disconnect between the concern of attacks and companies actually taking action. This Index will provide tangible insights into how threats are perceived at any given time, which will aid IT decision-makers in justifying vital cybersecurity spending to the board of directors," said Rodney Joffe, Head of NISC and Neustar Senior Vice President and Fellow.

The results of the inaugural survey completed in May 2017 show that:

- Sixty percent of respondents say recent global attacks, such as WannaCry have directly affected the way they have protected their own enterprise in the last six months.
- Respondents ranked ransomware as the most concerning with 28 percent of respondents selecting this type of threat, and system compromise ranked second with 21 percent. As the WannaCry attack crippled global systems, the positioning of ransomware as the top CISO concern is understandable and gives a

clear indication of current threat landscape awareness for this first Cyber Benchmarks Index.
- 44 percent of respondents have focused on increasing their ability to respond to both ransomware and DDoS, confirming that priorities for CISOs are avoiding both ransom requests and website disruption.

The International Cyber Benchmarks Index™ measures the level of concern in the NISC community of security professionals about the current international cybersecurity landscape and the index figure and survey results will be updated on a bi-monthly basis.

When asked if criminals were increasingly behind threats, 49 percent of respondents thought they were. When asked if they thought threats from unknowns were on the increase, 38 percent of respondents agreed. Responses from future surveys will reveal how the perception of the threat landscape changes over time, and currently show that threats are thought to be increasing most from the world at large (58 percent) and least from within a CISO's own company (30 percent).

"Understandably, security professionals have their finger on the pulse of the threat landscape, with the survey responses demonstrating their clear knowledge of attacks and attackers. Tracking who respondents think attackers are and where attacks come from will be interesting, as we will be able to see how global events and news headlines might, or might not, influence the answers," continued Rodney Joffe, "If news stories about election rigging lead to a rise in nation/state actors being considered a threat, then this will show up in the Cyber Benchmarks Index and provide a valuable regular touchpoint to take the industry temperature on cybersecurity. The results from this first survey taken in May 2017 have produced an initial index of 6.5, which is slightly elevated. Over the coming survey periods, we will track the rise and fall of concerns which will obviously be affected by both external events, and concerns internal to respondents' organisations."

The survey was conducted, on behalf of Neustar, by respected, independent market research agency, Harris Interactive. Director of Technology at Harris, Lee Langford, commented that, "The initial findings of this unique survey reflect a genuine concern about the threat landscape on the part of cybersecurity professionals across EMEA, and we look forward to working with the Neustar International Security Council to track security executives' opinions and concerns in this dynamic environment."

The Neustar International Security Council is an elite group of select cybersecurity leaders from key industries and companies, including business managers and senior directors, CTOs and other professionals with a security remit. Through face-to-face events including an annual summit, quarterly thought-leadership seminars and regional roundtables, members learn and share the latest trends from leading experts and peers. For more information: https://www.nisc.neustar/.

NISC Cyber Benchmark Index methodology

In May 2017, 290 interviews were completed across 11 countries: France, Germany, Italy, Spain, UK, Austria, Czech Republic, Netherlands, Russia, Switzerland and Ukraine. Survey respondents hold senior positions such as CTO, Director of IT and Security Consultant including business managers, senior directors, CTOs and other professionals with a security remit.

The Index figure is calculated using a number of questions that are to be repeated in every survey and tracked over time to create an index that is both stable but also sensitive to changes in the cybersecurity landscape. An initial figure is taken from the percentage of enterprises that say notable recent cyber events have directly affected the way they protect their business. This figure is multiplied by the average “net increase” percentages from across three separate questions (one which indicates how the threat of attack by various vectors has changed) (one which indicates how the risk of attack from various actors has changed) and (one which indicates how the threat landscape has changed).

Finally, Neustar multiplies the resulting figure by the percentage of enterprises that have ever been on the receiving end of a DDoS attack.??