Trend Micro Survey Confirms A Disregard for the Risk of an IoT Breach and Finds Loss of Trust As Biggest Potential Consequence

52% of businesses surveyed report loss of customer trust as the top consequence that would result from a breach
Two fifths (42%) of IT and security decision makers say security is an afterthought in their IoT strategies
Despite facing a growing threat landscape, only half (53%) cite IoT as a security risk

LONDON--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released survey findings that show businesses are most concerned about losing customer trust in the event of an Internet of Things (IoT) related cyber attack, however they remain unprepared. The survey, which was issued to 1,150 IT and security decision makers across the globe,1 indicates major discrepancy between the investment in IoT systems and security to protect them.

As the growing number of connected devices opens businesses up to additional cyber threats, close to half (43%) of IT decision makers and security decision makers say that security is an afterthought when implementing IoT projects (peaking at 46% in Germany). In addition, while nearly two-thirds (63%) agree that IoT-related cybersecurity threats have increased over the past 12 months (rising to 71% in the UK and the US), only about half (53%) think connected devices are a threat to their own organisation (75% in Japan).

Additionally, the results suggest there could be minimal testing taking place ahead of implementation to ensure new devices added to corporate environments are secured. The survey also showed businesses are experiencing an average of three attacks on connected devices in the last 12 months. Thirty-eight percent of those that have already implemented, or plan to implement, an IoT solution enlist security decision-makers in the implementation process. This falls to one in three for smart factory implementation (32%), with a similar proportion enlisting the help of security teams for the roll out of smart utility (31%) and wearables (30%) projects. This suggests that a significant proportion of businesses globally could be unwittingly opening themselves up to a range of threats.

“IoT systems are the future for businesses and many new types of connected devices are being introduced to corporate networks,” said Kevin Simzer, chief operating officer, Trend Micro. “While this is beneficial for business operations, the embedded operating systems of IoT devices aren’t designed for easy patching, which creates a universal cyber risk problem. The investment in security measures should mirror the investment in system upgrades to best mitigate the risk of a breach that would have a major impact on both the bottom line and customer trust.”

Security, responsibility, reputation, and business impact

According to businesses, the top consequences as a result of a breach include loss of customer trust (52%) closely followed by monetary loss (49%). Despite the recent introduction of GDPR making it top of mind for many, the following consequences were ranked significantly lower. Some of the areas businesses think an IoT breach would impact are:

- Customer trust (52%)
- Monetary loss (49%)
- Loss of personally identifiable information (32%)
- Being fined by regulators (31%)
- Breaking data security regulations (28%)

With breaches having the potential for a significant impact on business operations – such as jeopardising GDPR

compliance or taking critical networks offline – the research confirms that cybersecurity cannot be an afterthought and it must be key to the IoT implementation process from the offset.

Simzer at Trend Micro continued: “The significant investment in this technology across the globe is testament to the fact that IoT solutions can bring many advantages to businesses. But if security is not baked into the design of IoT solutions, and SDMs aren’t involved in the IoT implementation process, businesses could face damages far greater than the benefits this connected tech delivers.”

The findings show significant investment is going toward IoT systems, with businesses spending over $2.5 million on average each year. Given the substantial financial investment, and the significant impact to organizations that could come from a cyber attack against these systems, security must be equally prioritized to mitigate this risk.

About the research

The findings are based on joint research with Vanson Bourne. Between 1 April and 25 May 2018, 1,150 online interviews were conducted with IT and Security decision makers from businesses with 500+ employees in five countries, including USA, UK, France, Germany and Japan. Respondents held either C-Level, senior management or middle management decisions, and work in organisations operating in multiple sectors, including retail, financial services, public sector, media and construction.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com .

1 Research carried out by Vanson Bourne with 1,150 IT and Security decision makers across five countries, including USA, UK, France, Germany and Japan, between 1 April and 25 May 2018.

Contact:

Trend Micro Incorporated
Kateri Daniels, 817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

Additional assets available online: Photos (1)

https://newsroom.trendmicro.ca/2018-07-26-Trend-Micro-Survey-Confirms-A-Disregard-for-the-Risk-of-an-IoT-Breach-and-Finds-Loss-of-Trust-As-Biggest-Potential-Consequence