Media title: Addressing security risks from IoT
Author: Robert Trong Tran, Director of Cyber Security and Privacy Services, PwC Vietnam
Source: Vietnam Economic Times on 25 May 2017
Online link: http://www.vneconomictimes.com/article/op-eds/addressing-security-risks-from-iot

OP-EDS

Addressing security risks from IoT

Released at: 14:23, 25/05/2017

Mr. Robert Trong Tran (Photo: PwC)

Mr. Robert Trong Tran, Director of Cyber Security Services and Privacy Services at PwC Vietnam, discusses how organizations can protect themselves against security vulnerabilities in the Internet of Things (IoT).

by Mr. Robert Trong Tran, Director, Cyber Security Servicesand Privacy Services, PwC Vietnam

Vu Thi Thu Nguyet, Marketing & Communications Manager, Tel: +84 4 3946 2246, Ext: 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Media title: Addressing security risks from IoT
Author: Robert Trong Tran, Director of Cyber Security and Privacy Services, PwC Vietnam
Source: Vietnam Economic Times on 25 May 2017
Online link: http://www.vneconomictimes.com/article/op-eds/addressing-security-risks-from-iot

Last year's internet assaults by hackers commanding a hijacked army of connected devices - the latest in a series of record-setting distributed denial of service (DDoS) attacks - ought to goad organizations into reassessing how security vulnerabilities in the Internet of Things (IoT) may progressively jeopardize critical operations and networks. Instead of getting caught up in dread, uncertainty and doubt, though, corporate leaders can find a way to relieve these risks and gain the upper hand in the market place.

By targeting weak security on devices such as video recorders and routers and taking control of them in mass quantities, hackers have demonstrated that they can bridle and use the joined power of the frameworks as malicious robotic networks, dubbed botnets.

According to Dyn, an internet firm targeted on October 21, 2016, up to 100,000 malicious endpoints associated with the Mirai botnet unleashed a sophisticated DDoS attack that disrupted access to prominent websites in the US. The incident, which spurred an electronics maker to plan a product recall, was the "highest throughput DDoS attack seen to date," the Electricity Information Sharing and Analysis Center wrote in an October 24, 2016 white paper published online.

It appears likely that IoT-empowered dangers will turn out to be more successive and weighty. Organizations should be set up for situations in which moderately low-end hackers progressively have the ability to disturb digital trade.

In PwC's Global State of Information Security® Survey 2017, respondents said the average annual system downtime as a result of cybersecurity incidents was 20.2 hours. This number has been steadily increasing on an annual basis. Luckily, corporate leaders can ponder the risks from IoT and take strong actions to better secure key resources.

Resilience: First, we urge corporate leaders to prioritize resilience, which is key to thriving in the digital economy. A simple example of this would be using multiple DNS services rather than only one. Establishing business and continuity plans (BCP) can help reduce the risk of organizations being caught flat-footed, either in the event that mischievous hackers hijack mobs of connected devices in the outside world to disrupt business operations or if malicious actors target a particular organization's IoT with the goal of penetrating a network or physically harming others.

As the IoT expands, backing up data, raising employee awareness about cybersecurity best practices, including training to combat phishing attempts, and developing a comprehensive crisis response strategy is more important than ever. Companies that establish broad-based cybersecurity risk management efforts with automated security and privacy controls are better postured to sustain operations in the face of adversity.

Vu Thi Thu Nguyet, Marketing & Communications Manager, Tel: +84 4 3946 2246, Ext: 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Media title: Addressing security risks from IoT
Author: Robert Trong Tran, Director of Cyber Security and Privacy Services, PwC Vietnam
Source: Vietnam Economic Times on 25 May 2017
Online link: http://www.vneconomictimes.com/article/op-eds/addressing-security-risks-from-iot

Risk management: Second, the C-suite needs to devote increasing attention to IoT-related risks when discussing enterprise-wide cyber risk management. Corporate leaders are making some strides in this area. In PwC's survey, 46 per cent of respondents said that they plan to invest in security for the IoT over the next 12 months. Further, 35 per cent said they had an IoT security strategy in place and 28 per cent said they were currently implementing an IoT security strategy.

Nonetheless, there is a huge opportunity to become better. Organizations depending on IoT devices, especially those in critical infrastructure sectors, need to work to comprehend the size of the issue by stocktaking devices being used and deciding how best to designate speculations to enhance security and alleviate risks. This is particularly essential given the fact that hackers can spot IoT devices using an online searchable registry. The stakes are high for the healthcare sector, for instance, which has adopted medical IoT on a massive scale. Our research has shown that provider organizations have between three and ten connected devices per patient room.

Device security: Third, developers of IoT devices need to do a significantly better job of designing with security in mind. Designers ought to make it straightforward and reasonable for device users to acquire security updates as required. Devices should not include embedded passwords at the firmware layer that cannot be overwritten or decommissioned. They should include forensic logging and evidence capture capabilities, making it possible to determine indicators of compromise. Further, connected devices must be designed to operate in a hostile environment and to fail safely in the event they are infected with malware. Adversarial testing in the development process should be the norm. Further, devices should be designed to prompt users to change factory-default passwords that otherwise present easy targets for hackers.

In short, last year's major DDoS attacks should serve as a call to action for corporate leaders. Threats to the security of the IoT can no longer be disregarded or dismissed as mere nuisances. Organizations clearly need to better understand and address emerging IoT-related risks. That will require looking both inward and outward given the interconnected nature of the digital economy, industry's reliance on third parties, and the global nature of today's supply chains.