DATA PROTECTION

Salvatore Sinno *examines how public distrust in personal data use is stunting the Internet of Things market potential in UK*

The increasing variety of connected devices that people own and regularly interact with nowadays, is taking cyber security as well as its vulnerabilities into a whole new world of opportunity.

The cyber threat landscape is expanding and evolving, as criminals are also becoming more sophisticated and launching targeted attacks outside traditional signature and rule-set approaches at both individuals and enterprises of all calibres. As well as this, the variety of opportunities and routes for hackers to gain access to data is increasing, both in business contexts and throughout personal lives – with the variety of connected devices and systems individuals are interacting with regularly increasing, meaning large amounts of personal identifiable information is held by the average company.

SINCE 2014, THERE HAS BEEN A 40 PERCENT RISE IN OVERALL UK SECURITY CONCERNS

The sheer pace of knowledge and technical development of cyber criminals is the threatening factor to the public and business community alike, with the severity and detrimental impact of large cyber attacks seeming to rise with each case. We have seen ransomware distributed through phishing campaigns rip through international organisations and supply chains with perceivable ease as businesses struggle to react. Most recently, Petya Ransomware, exemplified the power of such attacks and highlighted how no organisation is immune to hacking attempts. The attack was active in over 65 countries and hit some of the most developed organisations in the world – Fedex, Reckitt Benckiser and Maersk to name but a few.

However, it is not just ransomware-based attacks that are concerning factors in the security landscape. In fact, a key area of concern is the manner in which designers and manufacturers of products, especially when considering IoT devices, secure, hold and utilise the data they gather from customers. Just earlier this year, CloudPets, which creates a successful line of internet-connected toys, was hacked, exposing 2 million voice recordings of children and parents as well as email addresses and password data from more than 800,000 accounts. The real issue with this is not so much the hack itself, it is more the poor security practice and lack of perceivable care the company placed in the data it was gathering. The account data was left in a publicly available database that wasn't protected by a password or placed behind a firewall.

Combine the consistent pressure from the hacking community targeting vertical industries with the fact that mainstream media has been devoting focus to highlight data breaches from household names such as the NHS, Talk Talk and the Houses of Parliament – average security concerns of the public are continuing to rise. In turn, this is playing a key role in the demand and perception of products, services as well as organisations and governmental services as they are brought to market and integrated into society.

A key factor for consideration that has been made even more apparent with the wider integration of connected devices into daily lives is the impact that control (or perceivable control) has in relation to average security fears around data privacy.

Unisys recently conducted its 2017 Security Index, which is the only recurring snapshot of security concerns conducted globally since 2007, and provides an ongoing, statistically robust measure of concern about security. Since 2014, there has been a 40 percent rise in overall UK security concerns, with internet security, which measures fears around viruses, hacking and online transactions, rising dramatically, up by 50 percent since 2014 – all linking to a lack of control in light of data access rights and security.

OPPORTUNITY KNOCKS

The rise of average technological capabilities of individuals, public awareness of common security threats as well as more access to security tools and solutions has certainly improved the ability for individuals to control their own security destiny to some degree. This envisages how individuals may be more effectively backing up data, carefully operating online to reduce vulnerabilities as well as ensuring common device security techniques are conducted.

Outside the Houses of Parliament may be well protected, but the hacking community has had some success targeting inside

Picture credit: Getty

As well as this, international and local governments are taking big steps forward to drive the control of personal data back into the hands of the public, forcing organisations to operate in a certain manner. Legislation such as the European Data Protection Regulation (GDPR) and UK Data Protection Bill will require organisations to manage, store and record consumer data much more carefully as well as hold a certain level of transparency – which will make big steps to reducing data privacy fears. However, control is still causing hesitation and raises questions of the current state of validity, transparency and need to access or track personal data.

Factors such as terror attacks, high-profile cyber attacks and the rising cost of living are all outside the public's control and they are major contributing factors to the Unisys Security Index registering record levels of concern in the UK. Steps to advise and protect the public, such as the launch of the National Cyber Security Centre, are moves in the right direction, but we need joined-up thinking across the public and private sectors to ensure the public are aware of risks, know how to avoid threats and act as securely as possible.

The UK public is seemingly selective about which instances of data access/sharing it is comfortable

▶

with when interacting with public services and products – depending on context as well as what organisation it is interacting with. For example, 79 percent of Brits were found to support using a button on their phones or smartwatches to alert police to their location during emergencies, however only 41 percent support police being able to monitor fitness tracker data any time to determine their location. This highlights a distinctly complex relationship between privacy, security and personal benefits, such as convenience to each individual when engaging with businesses or public services. Data such as location is inherently personal and must be considered that way by technology providers to improve the perception of trust in this exchange, as well integrating stronger assurance to the benefits of engaging in that manner.

The combination of people wanting to stay hyper connected and the growing number of high-profile cyber attacks and security threats is creating a society with high expectations of technology, but also with high concerns around how their personal data is used and managed. Technology providers need to continually educate and reassure consumers while providing transparency on security procedures and controls to protect users.

This high concern around the security of connected devices and the manner in which the public interacts with digital services highlights a need for technology and security providers to educate, reassure and provide clarity on security procedures for them to succeed and be fully adopted by the market. What it also makes clear is that trust is lacking more generally across the UK in how data will be accessed, used and shared.

BIG BROTHER IS WATCHING

The USI study reflects this feeling with just under half (49 percent) of the UK public indicating concerns that international and domestic intelligence services could listen to or watch them via their smart televisions and other smart devices. Just a few months ago, these concerns were made more of a reality with news that international intelligence services can and most likely will eventually turn televisions and smart devices into investigative systems to gain access to networks or user credentials when needed. The reality was further embedded when the technology and smart TV provider, in its privacy policy, warned its users that any information discussed around its smart TV would be captured and transmitted to a third party using its voice recognition service. In this instance consumers would be limited to the services offered by the TV if they did not want that voice data captured and shared.

The volatility of security standards and the seeming lack of clarity from governments and businesses in their capacity to utilise connected device data, caused over a quarter (27 percent) of the UK public to claim it would refrain from purchasing smart devices for homes due to the perceived threat of being hacked.

These consistent concerns around data access and usage will have implications on the wider adoption of connected devices to markets and it is therefore fundamental to look to overcome these fears. Gartner predicts that over 20.4 billion connected devices will be in use by consumers in 2020, meaning that 5.5 billion of them could potentially not be purchased or used by consumers in the first place due to fears of hacking. This means that $100bn+ could be at stake if consumers are not convinced about security robustness and capacity for data privacy.

Whether we are talking about IoT adoption, national security or how the public interacts with digital services, control and trust are two fundamental factors in the level of concern the public has in relation to it that needs to be addressed. By improving transparency between business, governments and the public and by emphasising any benefits from data sharing, perceptions and hesitation to interact with connected services will be reduced and trust will start be gained ●

> LARGE AMOUNTS OF PERSONAL IDENTIFIABLE INFORMATION IS HELD BY THE AVERAGE COMPANY

Salvatore is currently the Global Chief Security Architect at Unisys reporting to the Chief Trust officer & VP Global Security. He leverages advanced products, efficient managed services and vertical expertise to develop customised security architectures for his clients.

These internet connected toys were hacked, exposing 2 million voice recordings of children and parents