Collaboration in the digital economy: why working together is critical for growth

by Richard Parris, CEO & Founder, & Lubna Dajani, Chief Strategy Officer, Intercede

IoT services are beginning to deliver benefits to consumers and societies, as well as creating new markets and driving revenues across many sectors; from healthcare, education and agriculture, to manufacturing, transport and retail. The success or failure of the IoT will have a major impact on the growth of the digital economy on a global scale. However, the more dependent we are on our connected lifestyles, the more damaging cyber-attacks can be. Securing this ecosystem should therefore be an immediate priority and it's critical for all players to collaborate, at every touch point and each layer, to enable the IoT to deliver on its potential. This article discusses the security challenges and illustrates solutions and initiatives which will promote better collaboration throughout the market.

Richard Parris, CEO and Founder

Richard Parris is an Anglo-American technology entrepreneur with extensive experience in the cyber security and identity management industry. He founded Intercede in 1992 and has led the Group through all stages of its growth, including an IPO in 2001.

Richard regularly engages with governments and major corporations to promote the importance of identity assurance in cyber security, physical access control and the digital delivery of public services. He is a Chartered Engineer with an MBA from the University of Warwick Business School.

Richard is a member of Catalyst UK, a global network of influencers helping UK Trade & Investment, and the British government, to promote UK excellence internationally. He is also a member of the UK government's Cyber Growth Partnership.

Lubna Dajani is the Chief Strategy Officer at British digital identity and credentials management company, Intercede. She has over 25 years' experience in the digital and mobile technology industries, working with a variety of organisations from large corporations such as Microsoft, T-Mobile and Viacom to non-profit organisations and NGOs. Lubna has coined the term Allternet and regularly presents at industry events world wide on a range of issues including identity, authentication, mobility, data science and other leading edge technologies.

Lubna's keen area of focus is currently on securing the future of the IoT. She is a visiting scholar at NYU, the secretary of OTPA and the Co-Chair Marketing Council of the prpl Foundation, an organization focused on enabling the security and interoperability of embedded devices for the IoT and smart society of the future.

The recent WannaCry ransomware attacks affected more than 200,000 computers in over 150 countries across the globe, with victims including the NHS, FedEx and Telefonica, as well as police departments and banks. Ransomware attacks have been growing in recent years: there were an estimated 638 million such attacks last year, up from 3.8 million in 2015, according to SonicWall. The costs of WannaCry have yet to be fully calculated, but according to the same report, in the first three months of 2016, cybercriminals extorted $209 million from businesses and institutions using ransomware.

Attacks such as these should serve as a general wake-up call to everyone with computing platforms, including governments, corporates and consumers, to implement reliable security protocols, platforms, infrastructure and strategies to mitigate risk and shift our current culture.

A thriving digital economy - but highly insecure

The adoption of connected devices and development of connectivity technologies have helped to kick-start the now thriving digital economy. Smart devices are flooding the market, with 3G and 4G networks now available in a growing number of regions. The future roll-out of 5G will also play a vital role in powering new digital services and enabling the rapid growth of connected IoT devices. One report estimated that the value of the IoT to the UK economy alone will reach £62 billion by 2020. This is transforming life and work at scale, in both public and enterprise arenas.

While the proliferation of connected devices is continuing at a rapid rate, securing these connected devices remains a challenge. Furthermore, the lifecycle of a connected device and associated services is complex, involving multiple stakeholders and technologies. Weak or no security at any point can expose a device, user or industry to cyber-attack – highlighting why collaboration is now a must.

Threats to IoT

Many IoT device manufacturers, keen to get their products to market quickly, will often build devices with no, or poor, inherent security features, leaving them susceptible to attack. To date, implementing security at the device level is complex and expensive. While many of these gadgets, such as smart lighting, remote home access control and drones, appear harmless, many consumers fail to understand how such devices can be exploited by hackers if not properly protected. AT&T recorded a 3,198% increase in IoT vulnerability scans over the past three years.

The damaging fallout from connected device hacks has already been painfully demonstrated with a string of DDoS (Distributed Denial of Service) attacks in recent months. Hackers have repeatedly taken advantage of unsecured IoT devices, using these as entry points to flood servers with traffic, overwhelming resources, causing servers to crash, taking out services and creating losses for companies. The DDoS incident against Dyn in October 2016, which targeted connected printers and cameras, caused frustration for internet users and significant damage to the domain name service provider. DDoS attacks are estimated to cost up to US$40,000 per hour, on top of the reputational damage, disruption to users' lives and the potential loss of customer data.

If unsecured devices like those targeted in the Dyn attack can be hacked today, then what's to say that the autonomous cars, healthcare devices and critical infrastructure of tomorrow will not also be at risk? Whilst device manufacturers certainly have a role to play in securing these edge-of-network devices and applications, the success of the entire IoT-powered digital economy will only be guaranteed through the close collaboration and active participation of all parties involved.

Uniting for a trusted IoT

The good news is that collaborative work is now underway, as more parties recognise the need to impose stricter cyber security measures. This must now extend across the board from the early adopters to all regulators, policy makers, insurers and leading service providers as well as consumer advocates and educators.

Strong digital trust by design, from the silicon powering these devices, through all touchpoints and links in between, is needed to allow for the deployment and management of end-to-end trusted services. Open digital trust frameworks would allow individuals, organisations, devices and services to be identified, verified and authenticated from the point at which access is attempted.

The introduction of the General Data Protection Regulation (GDPR) which will come into force in May 2018 demonstrates the importance of such collaborations. GDPR is making collaboration and standardisation across industries, organisations and geographical borders not just a suggested goal but a legal requirement. This applies not just to EU member states, but also to those organisations located outside of the Union if they offer services or goods to, or monitor the behaviour of, EU data subjects, meaning the impact of the GDPR is global.

The prpl foundation is one organisation to champion the idea of uniting industry players, providing guidance to developers, manufacturers and service providers on APIs and frameworks needed to establish and deliver trusted services at all layers of IoT.

Efforts from a number of standards bodies and industry organisations have also marked a promising start to achieving the digital trust goal. These include the IoT Security Foundation, the Open Trust Protocol Alliance (OTPA), the Internet Engineering Task Force (IETF), and the Alliance for IoT Innovation (AIoTI). The aim of this European Commission incubated initiative is to strengthen links and build new relationships between the different players in the IoT from start-ups and SMEs to academics and research labs. These initiatives, and many others, are all promoting interoperability and convergence between standards by uniting often disparate parties.

Act now

We are without a doubt heading towards a digital age where people, products, and places will be more connected than ever before. Whilst this may enable an expansive new world of opportunities, it is also a double-edged sword. The IoT has the potential to encourage growth in the digital economy, but this will only be possible with the collaboration of all players involved. Working together to implement a chain of digital trust will mitigate the security risks which will otherwise stifle this growth, limiting the success of the digital economy of tomorrow.