IoT

PYMNTS.com AUGUST 2019

Intelligence of Things
Tracker

iROBOT ON CLEANING UP SMART APPLIANCE Security Risks

Feature Story (p. 7)

Vodafone to use IoT to monitor water shortages in Kent, U.K

News and Trends (p. 11)

The top IoT ecosystem players this month, including 10 additions to the provider directory

Scorecard (p. 17)

TABLE OF CONTENTS

PYMNTS.com
Intelligence of Things
Tracker

© 2019 PYMNTS.com All Rights Reserved

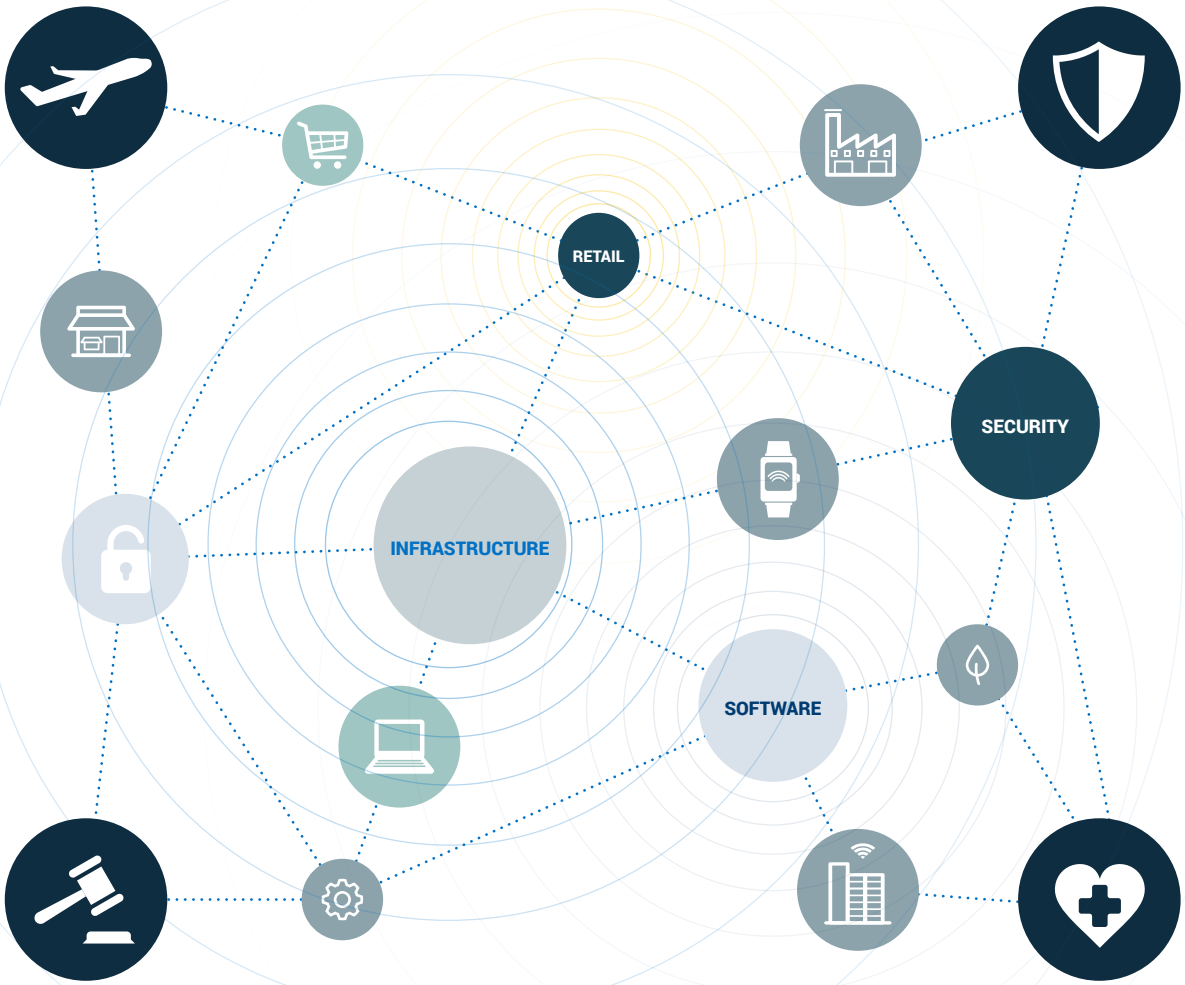
IoT ECOSYSTEM

SMART CITIES

Vodafone and South East Water partner to trial an IoT water leak detection system in Kent County, U.K. (p. 12).

SECURITY

Ninety-seven percent of surveyed IoT decision-makers said they had security concerns regarding IoT implementation (p.11).



LEGAL

A new U.S. bill will clarify which organization is responsible for setting federal IoT use standards (p. 15).

SELF-CARE

Shiseido has released a smart system that tracks customers' sleep patterns, home climate data and more to provide customized skincare regimens (p. 15).

© 2019 PYMNTS.com All Rights Reserved

WHAT'S INSIDE

There are more than 8.6 billion Internet of Things (IoT) devices in use worldwide today, and that number is unlikely to decrease. Consumers in Australia, China, the United Kingdom and the United States rely on such tools for everything from fitness tracking to grocery shopping.

Businesses and governments are finding more applications for the technology as well. IoT use cases outside of consumer purposes are becoming more of a reality, keeping factory floors running smoothly and tracking water shortages, among other applications. The U.K.'s Kent County is looking to the technology to manage water leaks as concerns over water use and shortages continue to grow, and Scotland's government is utilizing it to make an IoT-powered smart city a reality.

The technology is not progressing without struggles, however, and IoT security concerns remain prevalent — especially as numerous data breaches and device vulnerabilities are making themselves known to consumers and providers alike. These security issues are rapidly becoming a top priority for many in the industry as IoT adoption increases.

Around the IoT world

Microsoft has recognized these security problems and is now offering companies tailored solutions for their IoT platforms. The software firm recently launched dedicated IoT device protection as part of the Microsoft Azure Security Center. This will provide businesses with end-to-end protection for IoT, reducing fraud and cybersecurity concerns.

The IoT market is bracing for change in regulation and industry standards as different countries aim to shore up security. The U.S. government will soon present an IoT standards bill that will address and cover many of the industry's cybersecurity challenges. It will also clarify which organizations are responsible for creating IoT standards within the market.

The use of IoT for greater purposes is progressing, with cities like Chicago, Illinois, and Glasgow, Scotland, utilizing IoT technology to track air pollution. Both are using dedicated IoT sensors that give researchers and policymakers data on climate and air quality, helping them inform efforts to reduce pollution.

For more on these stories and other headlines from around the IoT space, visit the Tracker's News and Trends section (p. 11).

iRobot on cleaning up smart appliance security risks

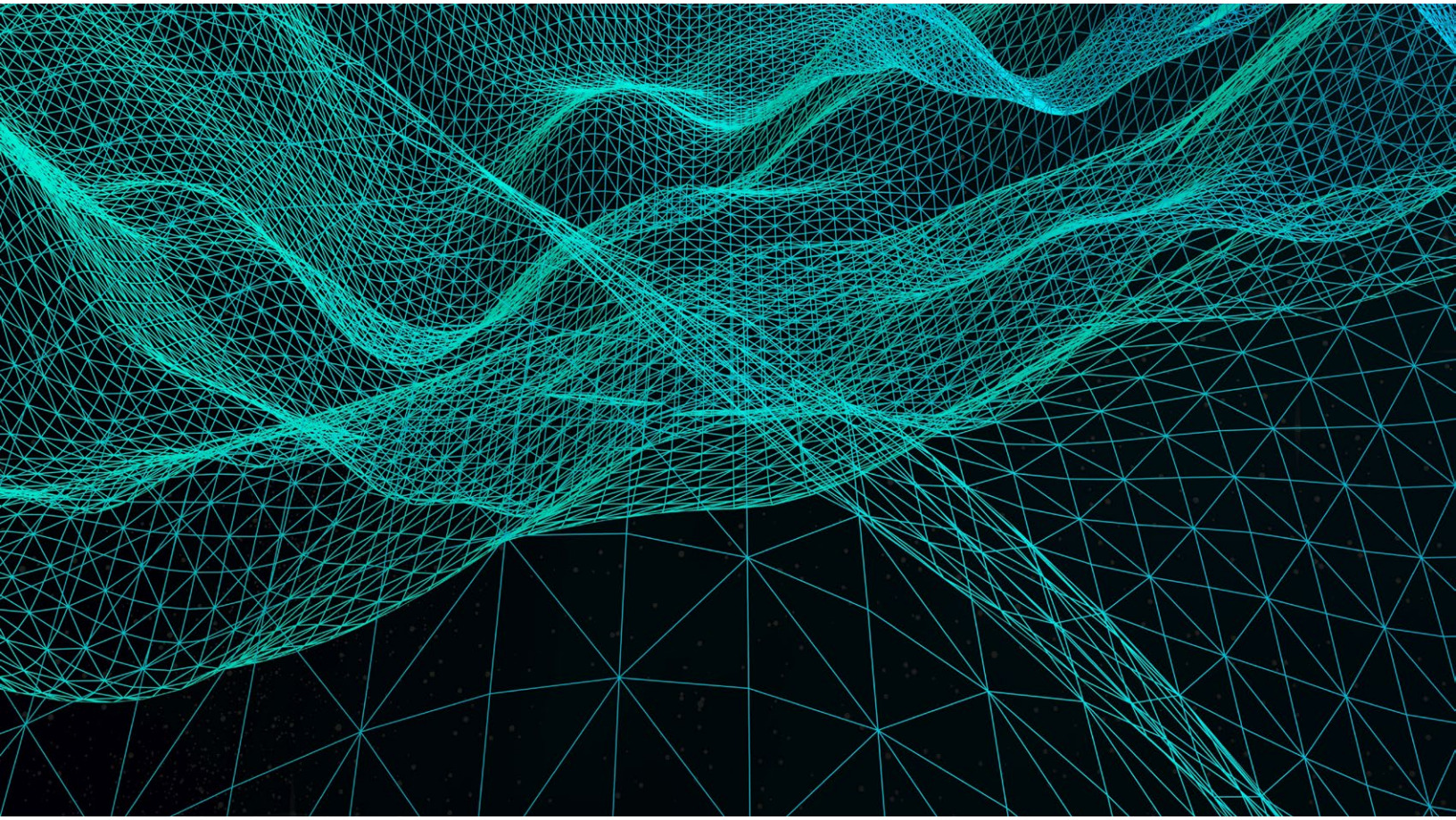
Smart home devices promise new levels of convenience and ease, but those benefits evaporate if they are left unsecured. Keeping devices secure requires continual vigilance, from the time of manufacturing to long after a products' release, according to iRobot vice president and chief information officer

© 2019 PYMNTS.com All Rights Reserved

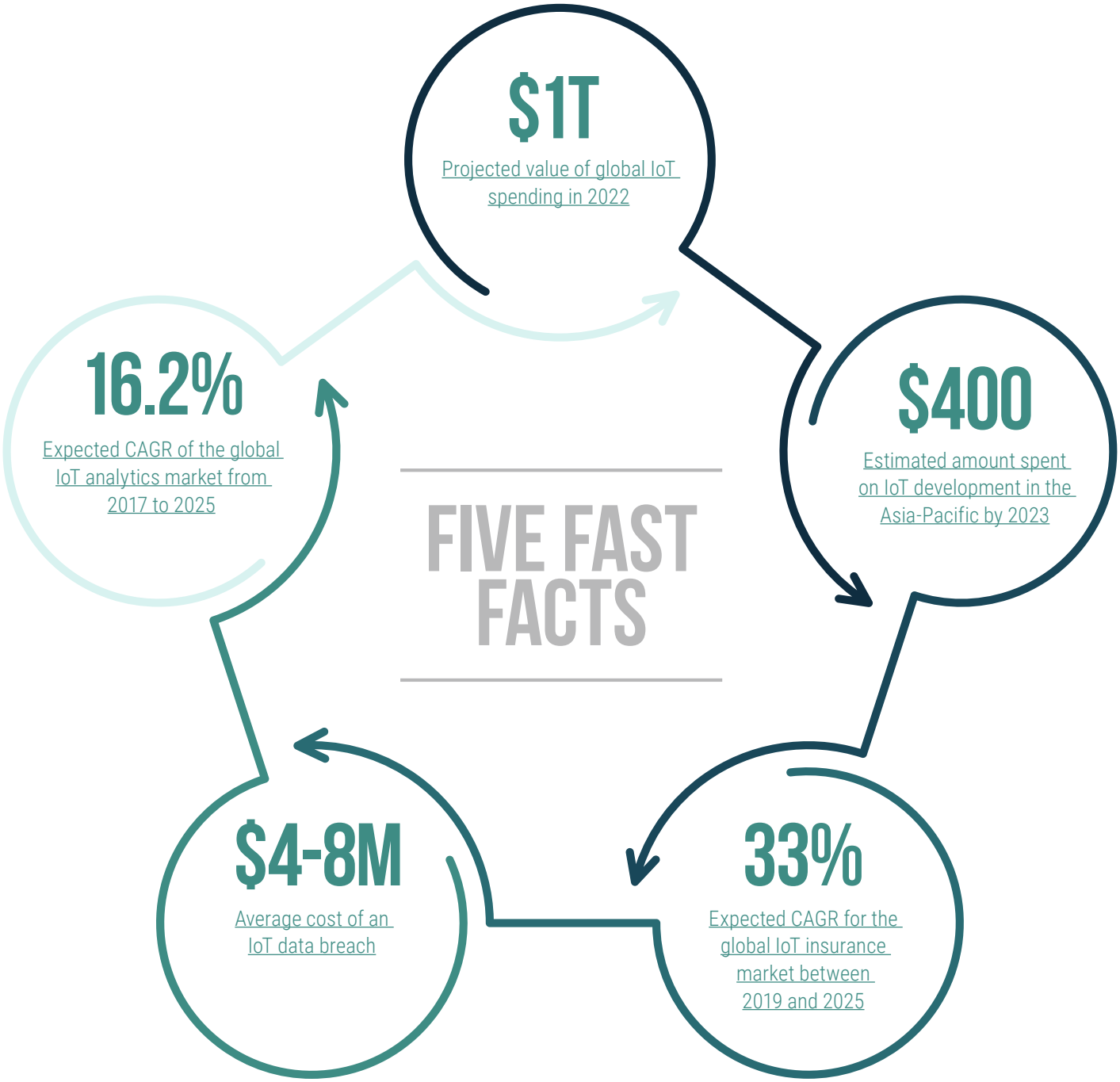
Mike Tirozzi and director of product and data security Mike Gillen. Companies should continually update software on deployed devices to protect against any new attacks that could emerge, they said, and work to safeguard them from vulnerabilities introduced by other smart devices that share the same home network. In this month's Feature Story (p. 7), the iRobot executives detail these and other pressing security challenges and strategies.

August Tracker Updates

The August Intelligence of Things Tracker includes a provider directory featuring more than 300 IoT implementers and enablers, including 10 additions: Gehring, John Deere, Kaeser Compressors, Karamba Security, Komatsu, KUKA, MachineMetrics, SCADAfence, SequoiaDB and Sight Machine.



© 2019 PYMNTS.com All Rights Reserved



© 2019 PYMNTS.com All Rights Reserved

FEATURE STORY

iROBOT ON CLEANING UP SMART APPLIANCE

Security Risks

© 2019 PYMNTS.com All Rights Reserved

FEATURE STORY

Home appliances have come a long way since the 1800s, when the electric oven and dishwasher debuted, or the early 1900s, when vacuum cleaners roared into middle-class American homes. Manufacturers promised these devices would ease the aggravations of housekeeping. They continue to work toward that goal a century later, in an age when "home device" conjures up a very different picture.

Smart appliance manufacturers leverage IoT technology to reduce the burden of home maintenance. These technologies may introduce conveniences, but they can also add new risks. Connected floor-cleaning robots may save residents lost time — and back aches — but they may be more trouble than they're worth if they're not secure. This is especially true given that traditional vacuums cannot become susceptible to cyberattacks.

PYMNTS recently spoke with home cleaning robot provider iRobot's vice president and chief information officer, Mike Tirozzi, and director of product and data security, Mike Gillen, on the ways smart home providers are tackling such issues and how providers can offer the conveniences of home IoT while minimizing risk.

Continual vigilance

IoT devices are exposed to potential cyberattacks for as long as they are connected. This means they need to be secured against the malware and other threats present at the time of manufacturing as well as those that may be developed long after the products are released. Device security is therefore not a one-and-done deal, but rather something that lasts the product's entire lifespan. Manufacturers must continually monitor and update their devices' software to stay ahead of evolving cyberthreats.

"We know that the landscape is going to change, the players are going to change [and] the attacks are going to change as well," Tirozzi said.

Both Tirozzi and Gillen noted that keeping software secure works best if the provider takes responsibility, as opposed to

© 2019 PYMNTS.com All Rights Reserved

expecting consumers to remember and know how to do so. All data transmission should be encrypted from the get-go and manufacturers should handle regular software patches and updates.

Intertwined security

Fraudsters can swoop in when security vulnerabilities are found and left unaddressed, compromising a device and others to which it is connected. iRobot seeks to prevent potential issues in which one hacked Roomba is leveraged to compromise others, and does so in part by giving each device a unique authentication for connecting to the company's cloud. It can then isolate a compromised robot and shut it down before hackers gain access to other devices or systems.

"[This] prevents more of a suite-wide compromise in the process," Gillen said.

IoT providers also cannot simply focus on their own products and IoT ecosystems. Tirozzi and Gillen explained that a vigilant provider's securely designed device can still be threatened if

© 2019 PYMNTS.com All Rights Reserved

it connects with a less-secure IoT offering, a problem that will grow as consumers place more connected items in their homes. Some may even be using smart solutions that do not receive security updates from manufacturers.

"You'll likely have connected devices where the company that makes them goes out of business," Gillen said. "[Those] devices aren't receiving updates anymore because the company doesn't exist, … but they're still connected in customers' homes. … Those devices may live on beyond companies' abilities to support them."

Companies can minimize opportunities for cybercriminals to interfere with their smart devices by taking several precautions. One common IoT security mistake is providing devices with default log-in credentials, which becomes a problem because bad actors can compromise all by stealing just one device's login. Consumers must also be capable of controlling how connected their devices are. iRobot's products can work with Alexa or Google Home, but only if the consumer actively chooses to link those accounts. The products are also capable of functioning offline, but making connections available as an "opt in" offering is key to giving consumers a sense of control and trust, Tirozzi and Gillen explained.

Consumers are increasingly turning to smart devices to enhance their home conveniences, meaning it is all the more important for providers to step up their security efforts. Those that want customers to regard their offerings favorably will need to ensure they can withstand attacks now and long into the future.

Under THE HOOD

What are your hopes for the future of the IoT smart home industry?

"The home is becoming like a robot in and of itself. What is a robot? A robot is something with actuators that can respond in real time; it can sense the environment, 'think' and act. As you see more connected devices coming into the home, the home is going to sense the person's needs and the person's presence and then act.

The home should do the right thing [by responding in a way] that's highly personalized for the occupants of that home. [For example], a widow who moves from Minnesota to Scottsdale, Arizona, may have different needs just based on the geography of her new home, versus a family of five in New England with four cats and dogs and a hamster.

Those homes need to respond and do the right thing in the space, and we have the hope that IoT devices built into and brought into the home will be able to do the right things for those individuals. … We're hoping to help that become a reality."

MIKE GILLEN

director of product and data security, iRobot

© 2019 PYMNTS.com All Rights Reserved

NEWS & TRENDS

IoT DEVICES AND SECURITY

Microsoft brings connected device protection to its Azure platform

Technology giant Microsoft is developing new solutions for IoT device protection as security concerns compound. The company recently launched the Azure Security Center for IoT, an IoT device security tool built into its Azure platform that will provide users with threat protection and security posture management tools. Michal Braverman-Blunmenstyk, chief technology officer for cloud and artificial intelligence (AI) security at Microsoft, noted it is designed for end-to-end protection.

Microsoft explained that the tool can protect against attacks on a wide range of IoT components, including sensors and edge computing devices. It will automate IoT security, including threat detection and response, taking work off clients' shoulders and enabling them to deploy the same level of security across all their IoT devices and components.

Security is the top industry concern for IoT professionals, study finds

Protecting IoT devices and data is becoming more of a concern as new vulnerabilities come to light. A recent study found that 97 percent of 3,000 surveyed IoT decision-makers reported having security concerns regarding IoT implementation. The development of strong user authentication was the most common issue, cited as a top concern by 43 percent of respondents. The next highest concerns were managing and tracking IoT devices and making sure device endpoints were secure, both of which were cited by 38 percent.

The study put the average cost of a data breach between $4 million and $8 million, meaning IoT security is becoming a top priority. Those costs only include the initial value lost in data breaches and do not take damage to the company's brand or customer retention into account. More than 8.6 billion connected IoT devices were in use as of 2018, and many more are expected to join.

IoT tech, mobile apps susceptible to 13-year-old encryption bug

Fraudsters are constantly coming up with new strategies and utilizing new technologies to break into IoT devices, but some older methods can still be relied upon. Research from Purdue University graduate student Sze Yiu Chau found that IoT devices and mobile apps are still vulnerable to an encryption bug that is now 13 years old. Chau noted at a recent conference in Las Vegas that such devices still have vulnerabilities related to the RSA encryption algorithm that protects virtual private networks (VPNs), emails and messaging, web browsers and IoT. The flaw manifests itself in signature validation of the encrypted data during the verification process. This allows bad actors to send in false data that appears to come from trusted sources.

Web browsers, mobile devices and IoT offerings remain vulnerable to the security bug as a result of developers using affected, prefabricated components without first checking them for potential cryptographic implementation problems. IoT developers and providers will need to exercise greater caution when utilizing prefabricated components in the future, and must keep protections in place for both older fraud methods and newer developments.

© 2019 PYMNTS.com All Rights Reserved

SMART CITIES AND DEVELOPMENT

Scottish government gears up for IoT infrastructure, development

Countries worldwide are looking at how IoT could best be applied within their borders, with Scotland's government recently sending out a contract notice to suppliers and businesses in the public sector concerning the development of the nation's IoT framework. It will accept applications for software, hardware, data analytics and security for the framework's development, and approximately 20 suppliers are expected to gain places on the project. The notice also states that the country's IoT development is still in its earliest stages, but the government expects to further push development over the next two years.

The contract notice follows other key IoT developments in the country, most notably last year's £6 million ($7.2 million USD) government program for the creation of a long-range, wide area network (LoRaWAN). The network will be designed to support IoT applications.

Tasmanian government invests $101K into energy, IoT accelerator

The Tasmanian Liberal Government in Australia is also investing in IoT, announcing a recent AUD $150,000 ($101,000 USD) investment into an energy and IoT startup accelerator that will support local technology startups and be led by CleanTech accelerator platform EnergyLab. Michael Ferguson, minister for science and technology, explained in a recent interview that the accelerator will help startups create and bring products

to market, and that startups will receive assistance with everything from hardware development and design to manufacturing and regulation.

The $150,000 investment is part of a total AUD $900,000 ($670,000 USD) Tasmania is set to spend on innovation. The government is also looking for partners and services to join its Start-up Accelerator program. Tasmania's is far from the only government investing in IoT, though. Those in the Asia-Pacific are set to invest nearly $400 billion into IoT by 2023, with other regions likely to follow suit.

Vodafone, South East Water team up for IoT water leak pilot

The U.K. is also leveraging IoT, implementing the technology to manage water shortages. Telecommunications company Vodafone is working with utility company South East Water to trial an IoT solution to reduce water leaks. The two companies

© 2019 PYMNTS.com All Rights Reserved

will trial the solution, which will use narrowband IoT (NB-IoT) sensors and digital water meters, for one year within Kent County. The "smart water" system will collect and analyze data, monitoring the state of the county's water. It will use "acoustic loggers" to listen to and zone in on leaks, which will be immediately reported to South East Water.

NB-IoT technology enables the system to run at low power, reducing the energy consumption of sensors and other deployed IoT devices and enabling their batteries to last for up to 10 years. The pilot comes as the U.K. is requiring the reduction of water leaks, as the region will be facing water shortages within the next two to three decades.

NEW SOLUTIONS AND TECHNOLOGIES

IoT and air quality, pollution reduction

Poor air quality is another problem some regions are hoping IoT can solve, especially given that air pollution is one of the leading risk factors for premature death around the world. Chicago's Array of Things project, which launched as part of a partnership with the Argonne National Laboratory, the University of Chicago and the City of Chicago in 2018, uses a system of 200 nodes to collect real-time data about the city's air quality and climate, among other factors.

© 2019 PYMNTS.com All Rights Reserved

Glasgow, Scotland, is moving forward with a similar project. The city's Sensing the City IoT project was developed in partnership between the University of Strathclyde and the CENSIS center for sensor and imaging systems and IoT technologies. It employs IoT sensor nodes to monitor air quality — including humidity, dust and carbon monoxide levels — and aims to better identify sources of pollution.

Universities race to fix IoT battery problem

IoT sensors monitoring water leaks or air quality in remote areas are only useful if they have adequate battery life, however. Universities and private entities are now looking to create better solutions to power such devices. Scientist Jerry Luo from the U.K.'s Cranfield University is studying the application of energy harvesting for IoT power, while Silicon Valley-based entity Alta Devices is developing a solar-powered solution for more IoT energy. These researchers and companies are working on the assumption that traditional batteries will inadequately meet the energy needs of future IoT devices.

CertNexus teams ups with IoT Community over skills gap

Emerging technology certification provider CertNexus has partnered with member-based organization IoT Community to address the gap between the need for IoT talent and the talent pool itself. IoT Community focuses on commercial deployment of connected technology, and the partnership will provide industry workshops and training solutions for an ANSI/ISO 17204-accredited IoT certification, the Certified Internet of Things Practitioner (CIoTP). CertNexus will provide such modules to IoT Community's more than 24,000 business and IoT specialist members, while also granting them access to other micro-credential services such as virtual classes, labs and digital textbooks.

The partnership comes as more companies look for developers, security officials and others who can work with and shape the developing IoT world. A recent study found that 76 percent of companies surveyed currently need senior staff with IoT-related skills. Such skills could be applied to a variety of

© 2019 PYMNTS.com All Rights Reserved

industries, including healthcare, infrastructure and insurance. IoT for insurance is predicted to expand at a compound annual growth rate (CAGR) of 33 percent between 2019 and 2025, reaching more than $9 billion by 2025.

Shiseido debuts IoT-based personalized skincare system

Japanese beauty and personal care company Shiseido has created a skincare system that relies on IoT technology to track consumers' sleep patterns and living conditions, including temperature, humidity and other data. Those details are then sent to dedicated customer apps for analysis before the tool recommends customers' personalized skincare regimens. The technology is available through an Optune subscription, which Shiseido says recommends any of 80,000 separate skincare regimens.

The global cosmetics market is expected to reach a value of $805.6 billion by 2023. Companies looking to rake in a greater share of these profits are likely to innovate and implement similar IoT solutions.

IoT STANDARDS AND LEGISLATION

US preps for IoT legislation, thanks to bipartisan house bill

The U.S. is introducing measures for improved cybersecurity with a bipartisan bill surrounding IoT security and fraud threats. The bill clarifies several points of confusion, most notably which organization is in charge of setting standards for federal IoT use. The bill names the National Institute of Standards and Technology (NIST) for this role, mandating that it update and continuously report these IoT standards. It also requires that vendors selling IoT devices and technology to the federal government self-report cybersecurity and other fraud problems, and that federal agencies will only be allowed to purchase devices that follow the NIST standards.

This legislation could go a long way toward preventing security problems accompanying federal government IoT use, mainly because it would finally create standards within the market as well as policies and procedures for device manufacturing.

IIoT standards face interoperability challenges

Industry standards for IoT devices still need to work through several challenges, though, one of which being current devices' interoperability. Standards will need to fit devices that are working across different industries, applications and communication channels, for example. A number of industry bodies — including the Industrial Internet Consortium (IIC), the Object Management Group (OMG) and One M2M — are working to set standards for machine-to-machine (M2M) communication in industrial IoT (IIoT). These organizations are considering the best ways to develop such frameworks, including whether they should be open standards. Huei Sin Ee, vice president and general manager of general electronics measurement solutions at Keysight Technologies, said in a recent interview that open IoT standards are advantageous because they draw on existing skill sets and support integrating legacy factory systems with new technologies.

© 2019 PYMNTS.com All Rights Reserved