IOT: THE NEW TACTICAL AND THREAT EDGE

Just a few years ago, Samsung's push into 'hyperconnected-tech' was highlighted by an expensive 'Internet of Things (IoT) City', arrayed in a large area inside the vast Consumer Electronics Show in Las Vegas.

GORDON FELLER | US

THEIR cutting-edge IoT innovations, intended for use by many kinds of organizations, were prominently featured. Since then, at each new CES event, Samsung has continued to showcase these kinds of products and services. They do so alongside hundreds of other big-tech companies, to the evident delight of the 180,000 gathered in Vegas.

CES in 2020 was no different, although this year there were some strong notes of hesitation. Why did so many seem so worried? The answer, in one word, is security – especially the security of all manner of 'IoT endpoints' and connected devices. The defence technology community is worried about vulnerability of smart-data transport, moving from the edge to the cloud. For this reason many are now questioning the emergence of IoT, and re-assessing its potential.

Despite the hype that 'anything IoT' has prompted over the years, a growing number of organizations in government and industry have begun to show genuine hesitation before diving right in. This is largely due to growing awareness of IoT's unique security threats. Organization leaders now know that they must understand how to secure IoT endpoints and devices while enabling data transport from the edge to the cloud – with insights delivered to customers at the end of the process.

The second biggest DDoS attack - as listed on Cloudflare's 'Famous DDoS Attacks' website - occurred in October 2016. That attack was directed at Dyn Corp., a big US-based DNS provider. As summarized by Cloudflare's executive team, the attack was "devastating and created disruption for many major sites, including AirBnB, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub". This was done using a malware called Mirai. It creates a botnet out of "compromised IoT devices such as cameras, smart TVs, radios, printers, and even baby monitors. To create the attack traffic, these compromised devices are all programmed to send requests to a single victim".

SOLUTION SPACE

What are tech leaders to think in 2020, especially as they run the varied kinds of organizations, large and small, that become cyber-targets – companies, governments, universities, hospitals? Each of the major tech companies has a white paper that aims to answer that question.

A group of world-class experts have been consulted to share their views. Here are a few of the key insights that we learned from them.

When he served as Deputy Director of Cybersecurity at the US Department of Homeland Security's Science & Technology Division, Scott Tousley was based at headquarters in Washington, D.C. He now serves as Splunk's Senior Executive, Cyber Programs. Tousley was concerned about the risks associated with "these needed new capabilities , because of lagging governance practices."

"Security governance approaches are not now quick enough, or adaptable enough, to support effective identification, management and reduction of risk, as these new capabilities develop and deploy," Tousley said.

He predicts that "we will continue to see many different threats actively attack these distributed and often haphazard environments". Why is he so worried? Because the tech industry has created environments that are governed by different organizations and technologies and approaches. Tousley is witnessing a situation wherein we're all 'outdriving our headlights' because the industry "designs and deploys and operates more rapidly than our risk understanding and governance can keep up with".

There are a host of different threat organizations working every day, out there in the real world. Some are small, and some have larger teams and organizations. They're based out of many different countries and regions.

"THREAT ORGANIZATIONS SEE A TARGET RICH ENVIRONMENT - AND RETAIN WHAT TOUSLEY CALLS THE "ADVANTAGE OF INITIATIVE", INSOFAR AS THEY CAN CHOOSE WHEN AND WHERE TO GO AFTER PARTICULAR TARGETS."

LEFT: More and more parts of the supply chain rely on internet enabled devices.

GETTY

All these actors are actively conducting reconnaissance, to aid them in deciding what targets to go after. These actors then choose their target, attacking in ways that are increasingly sophisticated. Tousley thinks that these attacks will increasingly focus on "IoT environments, which are not very tight/defined enterprise environments." He considers these to be more distributed, haphazard, ad-hoc, normally governed by different organizations and technologies and approaches.

TARGET RICH ENVIRONMENT

These different threat organizations see a target rich environment--and retain what Tousley calls the "advantage of initiative", insofar as they can choose when and where to go after particular targets.

IoT technologies put into production quickly become a critical piece of organizations' value chains. Organizations must automatically apply the same approach, products and technologies that they use for security and privacy compliance to the IoT devices when they introduced into the operation processes, said Bjorn Andersson, Senior Director of Global IoT Marketing at Hitachi Vantara.

Rob van Kranenburg, Founder of The IoT Council (theinternetofthings.eu), predicts that the next decade will be characterized by "fights over the core addressability and unique identifiers of people, objects and events". He sees us, in 2020, on brink of 'a Google moment': the first Google webpage "charmed users with its clarity, simplicity and performance. We can now see it as a 'Trojan Horse', porting large datasets and value". van Kranenburg argues that Google as a search engine was, from the beginning, not an end in itself, but an enabler.

The original internet framework, as described by Bob Kahn and Vint Cerf, was what van Kranenburg calls a distributed, decentralized but hierarchically structured marketplace. Their systems-approach "envisioned IoT situations where not only natural persons, but machines, robots and sensor enabled objects would need to be searched and found."

Wearables, smart homes, connected cars and smart cities are all connected systems balancing processing of information in the Cloud and (more and more) at the edge (on the devices themselves). The main difference between the web and IoT of today is this, in his view: "instead of a client which can be a person or a connected object actively pulling for data and information, the data, information, and services get pushed to clients that expose their wants and needs in a coherent way."

ADOPTION EVOLUTION

Kim Zentz, Urbanova's Executive Director, is deploying IoT devices in the field in Spokane, Washington. She thinks the real threat to enterprise security.

"In any type of field deployment of technology, rests with the clear, consistent and factual communication with all of the people involved," Zenta said. "This includes the employees in the office and in the field as well as customers or clients and those who may interface with the technology in a tangential or sporadic fashion."

As Zentz and Urbanova push forward, they've concluded that people are now ready and willing to adopt changes at varying paces:

"Technology deployments must build the human factors into the schedule. These steps cannot be rushed without compromising the security of all involved."

Zentz and her Urbanova team believe that it's best to start at a manageable scale.

ABOVE: The separation of work and home devices is blurring with increased integration.

"Adapt to the lessons learned before expanding the deployment."

It's noteworthy that this approach is driven as much by security concerns as it is by another consideration.

PROTECTION BY DESIGN

In order to provide an impartial guide to IoT security, the team at Arm, one of the world's largest chipmakers, commissioned a white paper, "Securing IoT Solutions by Design". The paper was authored by David Rogers MBE, an IoT security expert and founder of Copper Horse Ltd. Rogers is certainly a world-class choice: he chairs the Fraud and Security Group at the GSMA, serves on the Executive Board of the Internet of Things Security Foundation, and was awarded the MBE for services to Cyber Security in the Queen's Birthday Honours 2019. Among other things, Rogers argues that "IoT system developers should be looking for supplier who can provide a level of assurance that the supplier makes things easier for engineers to work with and the supplier keeps on the top of the security concerns at a detailed level".

"TECHNOLOGY DEPLOYMENTS MUST BUILD THE HUMAN FACTORS INTO THE SCHEDULE. THESE STEPS CANNOT BE RUSHED WITHOUT COMPROMISING THE SECURITY OF ALL INVOLVED."

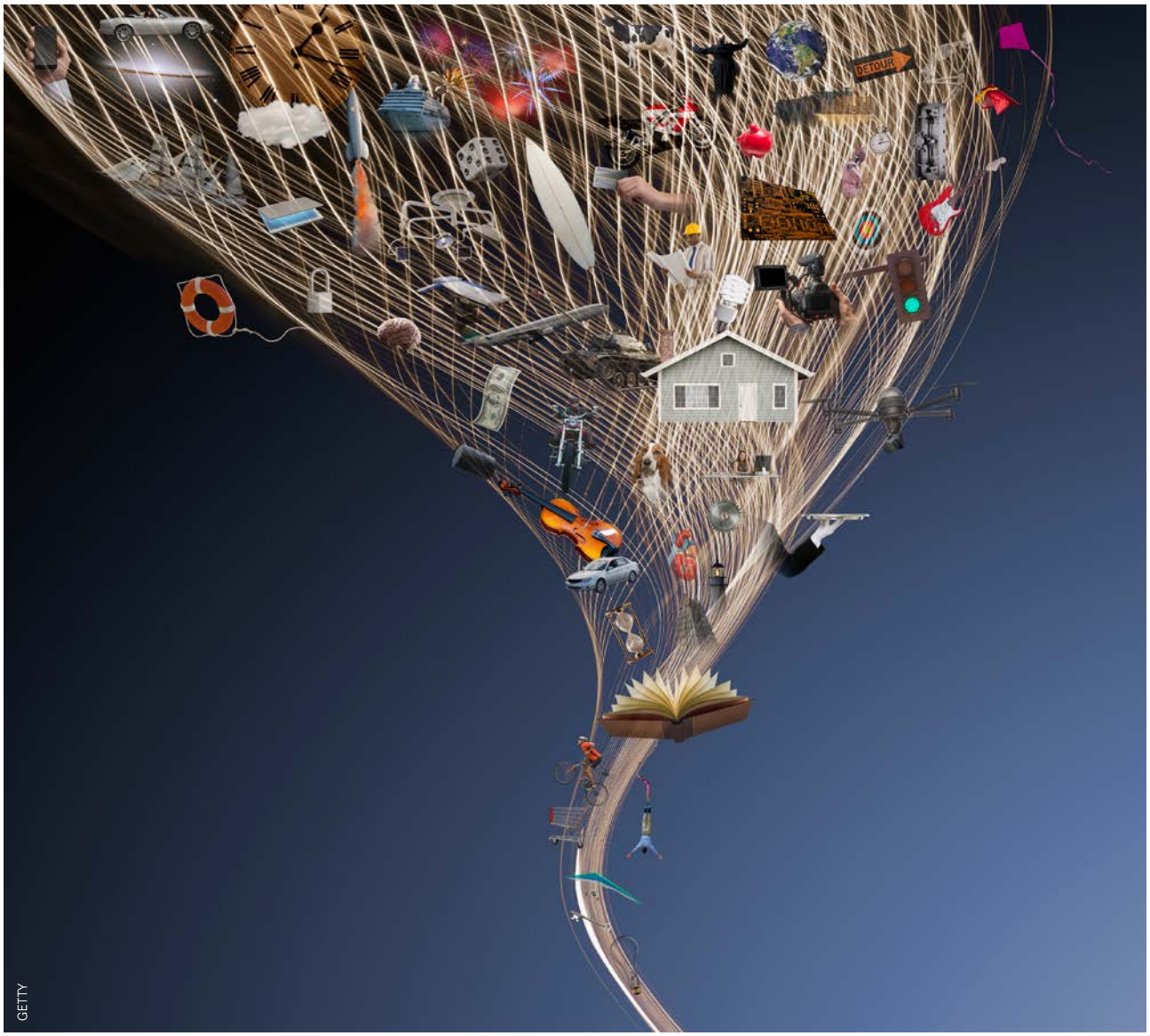
Despite the hype that anything IoT has prompted over the years, organizations have begun to show some hesitation before diving right in due to growing awareness of IoT security threats.

Organizations must understand how to secure IoT endpoints and devices; data transport from the edge to the cloud; preventing Distributed Denial-of-Service (DDoS) attack ... attacks; how an attack gets by security; patching holes.

DDoS attacks are defined by Cloudflare as a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Speaking to some of the world's leading IoT experts for their advice about what they and their organizations think about the biggest threats to IoT deployments we asked the following questions: Which of the different types of threats are worrisome (such as malware, botnets or DDoS attacks)? How can organizations mitigate them?

According to Nima Baitai, Lenovo's Director of Cybersecurity Solutions in their Intelligent Devices Group, IoT (and connectedness to the digital network) "continually shapes and touches every facet of our lives and how we interact and experience the world around us.



GETTY

"A COMPANY DEPLOYING AN IOT NETWORK NEEDS TO CONSIDER POSSIBLE ALGORITHM HACKING SCENARIOS, AND IMPLEMENT ALTERNATIVE COUNTERMEASURES STRATEGIES IN THE ALGORITHM DESIGN AND TESTING."

The security implications of IoT mean that malicious actors can leverage these devices for attacks with far reaching impact."

Nima thinks that the so-called Mirari botnet mentioned earlier was a watershed moment for IoT security. In that instance in 2016, an attack used IOT devices to launch DDoS attacks at a global scale previously unseen to bring down major services and even target government networks, such as Liberia's internet infrastructure.

Nima's focused on the continued growth of IOT devices both in the consumer and commercial arenas, wherein "the potential impact of such attacks continues to grow. As such, it's incumbent on organizations to increase their diligence of ensuring they have visibility into what devices are connected to their critical networks and to apply security controls to those devices."

One of the great challenges can be, as with Mirari, that the concerns reach beyond the devices connected to our own networks but also to how we mitigate risks posed by the potentially billions of devices outside our organization that can be compromised and used against critical networks.

"Having network redundancies, continuity plans and proper segmentation are vital," Nima said. "Ultimately, we, as consumers must also look to the device manufacturers to place greater emphasis on building-in security to these devices. That is economically challenging given the hunger of consumers for more and more devices at lower and lower prices. There is no silver bullet. It will take a concerted effort across vendors, regulatory agencies and organizations working together to address the security challenges of IoT."

THREATS

For a somewhat different point of view, consider the perspectives of Craig Williams, Director of Outreach at Cisco Talos.

"The biggest threat to IoT deployments is the fact that these devices - our cameras, our thermostats, our

dishwashers, our smart refrigerators, and even the locks that secure our homes are now computers," Williams explained. "Like any computer these have security issues which will be discovered and exploited by hackers. Cisco Talos has discovered these types of issues and worked with venders to patch them so that attackers lose the safe haven they could otherwise utilize to move laterally throughout the network with relative ease. Everyone considers security a priority until it adds $20 to the cost of a device - then suddenly the one on sale no one has heard of looks more compelling."

Benson Chan, Senior Partner at Strategy of Things, notes that IoT networks deployed in the field are vulnerable to a variety of security threats.

"Many of these threats breach the devices in order to gain access to the network," Chan said. "But another equally dangerous type of threat involves 'hacking the algorithm' behind the devices without breaching the device itself."

These attacks are designed to create uncertainty and mistrust in the algorithms. Once such trust is lost, you wouldn't use that device in critical situations. Benson concludes that "a cyberattack doesn't always have to cripple the network, sometimes all it needs to do is to slow someone down temporarily or take away someone's competitive capabilities."

Analogous to this type of attack would be painting over the words "Stop" as it appears on common stop signs on busy streets. An autonomous driving vehicle, equipped with a variety of IoT sensors, is programmed and trained to stop the car at an intersection when it detects the word "Stop" on a red octagon sign and on the street. However, this simple hack tricks the sensor into misclassifying the intersection as "no stop".

DEFENCE OF IOT

Benson thinks that defending against these types of threats is not easy.

"A company deploying an IoT network needs to consider possible algorithm hacking scenarios, and implement alternative countermeasures strategies in the algorithm design and testing," Benson said.

In the stop sign scenario, one possible countermeasure is to look for a stop sign on the opposite intersection. If one is detected, it is highly likely that this is a "stop" intersection. That said, Benson believes that there are many ways an algorithm can be hacked (some known, but most unknown), and companies would be advised to set up a rapid deployment capability in order to respond quickly to these hacks, as they arise, and mitigate them in near real-time.

GETTY

From his vantage point in Washington, D.C., Josh James of the law firm Bryan Cave Leighton Paisner says that the greatest threats posed by IoT devices on any network "are the increased surface area for attacks -- and organizations' failures to think about connected devices as tiny computers that need security".

Each IoT device adds a new vector for attack.

" This needs to be accounted for by an organization's security team; but that's not something that most organizations budget or plan for when they're thinking about adopting a new smart coffee maker or connected TV in the office breakroom," James said.

Additionally, depending on the location of the devices (if shared with the company's customers on a sales floor for instance), their physical security may present issues that a tech team doesn't normally have to address. To tackle these issues, James thinks that it's important for organizations to treat connected devices like other computing equipment and to run their acquisition through the organization's normal processes for addressing new network hardware—that's just not something folks consider when they order new thermostats.

"IOT IS AN ENABLER OF A TRANSPARENT SOCIETY THAT GIVES INDIVIDUAL GOOD AND TIMELY FEEDBACK ON THEIR IMMEDIATE CONDITION AND SURROUNDINGS IN WEARABLES. "

"With consumers and citizens becoming more dependent on services enabled by IoT devices, robust security is paramount to maintaining digital trust - the linchpin of the end-user experience," according to Sridhar Rao, VP of Engineering and Product Management at TCS Digital Software & Solutions Group.

Rao is concerned about the situation in 2020: "As more devices deliver data insights that shape real-time customer experiences, addressing IoT security at the device level becomes impractical. IoT security must be a holistic component of system design – spanning hardware, networks and applications -- instead of an afterthought to be addressed later. It's the only way to ensure reliable and secure connections that protect your business and customers."

LEFT: Cloud based technologies are providing both opportunities and challenges for many organisations.

EDUCATION CAMPAIGN

van Kranenburg says that the biggest threat to IoT applications is the "miseducation of the general public", fueled in part by gadget reporting. He worries about the fact that "the security industry has a stake in hyping security issues", since this is a business model. He argues that IoT is an enabler of a transparent society that gives individual good and timely feedback on their immediate condition and surroundings – and thus we have wearables. IoT provides for smart and cheap resource management in our homes, for better public and private transport using our connected bikes and cars, for downsizing of overhead and for coordinated collaborative smart procurement in cities. He argues that this is not a fairy tale.

"The one biggest threat to IoT applications is IoT applications," van Kranenburg reflected.

He argues that it's vital for engineers to protest against the loss of privacy, but that they must stop merely lamenting this; they must start to join forces, in order to build the best possible connected worlds.

"It's perfectly possible to build the ideal balance between national/regional centralization of infrastructure, full decentralization of services and data staying with people," van Kranenburg said.

This would mean a kind of edge environment, one where the router becomes an important and highly secure element in validating assets and devices connecting with and through the router.

Is there some good news out there, especially for those in tech who're undertaking IoT deployments? One small sliver of light emerged in January 2020, when the US Senate passed what some consider to be the very first Federal bill focused on IoT. In an Australian context, the legal frameworks have yet to catch up to the endless opportunities, both good and bad, of the IoT world around them. ■