Cyber security
in the augmented age

By Gary Maidment

Connectivity is increasing and will continue to do so as the first nations stride into the hyper-connected stage of Augmented Innovation. Huawei estimates that there will be 100 billion connected devices by 2025, which in turn will create a considerably larger playing field for digital crime. John Suffolk, Huawei's President of Cyber Security and Privacy, shares his thoughts on this vitally important facet of today and tomorrow's world.

Telling it like it is

In July 2015, Symantec CTO Amit Mital declared that, "Cyber security is basically broken," a sentiment with which Suffolk agrees, in part because technology has a history of outpacing our ability to secure it: "PCs were invented 35 years ago, and we still haven't got the ability to fully secure them," he points out. Given that security and privacy issues don't discriminate when it comes to tech, the fact that it's extremely tough to make any system 100 percent secure is likely to hold true in the future.

Not quite enterprising enough

Hacked enterprises regularly make the news, and will continue to do so if vulnerable or outdated IT equipment remains prevalent. High-profile attacks last year included the toymaker VTech, where hackers compromised the data of 6.8 million children and 4.9 million adults – the largest cyber attack involving children ever. A significant data breach last October saw the entire data cache from the crowdfunding service provider Patreon published online, affecting millions of accounts and involving gigabytes of data and code. And last year, attacks on multiple financial institutions were found to be connected, allegedly laying the groundwork for stock scams before the perpetrator was caught. Affected firms included JP Morgan Chase, which had 83 million customer details stolen, and Scottrade, which saw the data of 4.6 million customers compromised.

Stuck in a timewarp

Alongside vulnerable equipment, enterprises are also at risk because today's tech environments are increasingly complex, and the boundaries of where your tech starts and ends are indistinct, "Many security experts talk of an attack surface," says Suffolk. "In this new world you can't see the edge of the technology your company might be using, so how do you defend what you cannot see? The current and future world is much more complex – it's all about sub- and cross-border systems and ecosystems."

While the environments in which technology exists are moving forward, approaches to cyber security are lagging behind. "By focusing on protecting single products, the ICT industry and policy makers are stuck in the 1980s," says Suffolk. "Standards like PCI, FIPS, TL9000, Common Criteria, and ISO management systems are useful, but they focus on a single product or system and that simply isn't enough."

The Internet of Hackable Things?

And it's not just enterprises. The nascent world of IoT is seeing more products connected than ever before, and greater device visibility ramps up security risks. Low-cost devices may not see as much investment in security measures, and the design efficiency of smaller-capacity, low-power devices restricts some of the options for security countermeasures. This creates the risk of so-called zombie IoT botnets that could potentially affect networked systems like CCTV surveillance cameras and medical devices. Last year, two hackers demo-hacked a Jeep Cherokee for Wired magazine, causing Chrysler to recall 1.4 million units after the hackers remotely took over dashboard functions, steering, transmission, and brakes.

When discussing Mital's comment about the state of play in the cyber security world, Suffolk is quick to point out the root cause: "It's not just that cyber security is broken; our approach to risk management at a government and corporate level is broken. "This, he says, is due to the interplay of multiple factors: "The complexity of technology products and systems, business commercial pressures, cloud computing, and international laws, and not having a model for assessing a complex risk position that can quickly shift."

Look to the layers for answers

But, it's not all doom and gloom. Suffolk advocates a risk-based, layered approach to cyber security that recognizes that some data must be 100 percent secure, or at least as secure as we can make it. "The issue is how secure do I need to be for the service I'm providing or receiving?" he says. "Not all systems, or data, are born equal; for example, health data is more important than your shopping list, air traffic control is more important than your games console."

Suffolk is clear that we can't treat everyone the same in a world of 5G, cloud, and IoT. Because of the blurry nature of current and future attack surfaces, he asserts that security must be layered, zoned, or segmented because you can't pick a single best approach when one size definitely doesn't fit all. While verticals are good at managing their own technology, the challenge, Suffolk says, comes when you connect to different clouds from multiple service providers using a range of BYOD and work devices, because you don't always know what cloud or infrastructure you're connecting to.

Another must is ensuring that security measures are built-in and not bolted-on. According to Suffolk, this is starting to happen, "Vendors are working hard to improve product security, and standards bodies are building better security designs, such as north bound interfaces for IoT, which builds in protection when technology components start talking to each other."

Equally important for enterprises, this built-in security approach needs to exist in a seamless and complete context. "We're focusing on an end-to-end approach to security and privacy across our complete product portfolio," states Suffolk, "from design and build to deploy and maintain."

Prevention is better than cure

In the current state of play, experts like Suffolk are pushing cyber security in the right direction, layering new technologies as the armor in the augmented age and using agility as the spear. Advancements have been made in cloud, big data, analytics, and high-performance computing, which can cover much more ground when acting in concert to protect systems and networks. "Computers are much better than humans at looking at vast amounts of data and working out anomalies in patterns," explains Suffolk. "We're doing that with our next-generation security products, such as firewall and anti-DDoS, connecting through cloud and using big data to be more insightful."

The reality of cyber threats that span boundary-less attack surfaces requires that security measures are agile, risk-based, and layered. In Suffolk's words, "You need to understand what the key assets are you want to protect and how to protect them – all of that is a journey, and in a time of dramatic technological change, a journey with no end." WIN

Wagenia man fishing in the Congo River

HUAWEI

intel CORE m7 inside

The new style of business

HUAWEI MateBook

Ultra slim & light | Long lasting | Portfolio keyboard | Versatile MatePen

MAKE IT POSSIBLE
consumer.huawei.com

Product colors, shape, interface and the functions are for reference only. The actual product may vary.
Demonstration is created by visual effect. UI functions and applications may vary by region.
Intel, the Intel Logo, Intel Inside, Intel Core, and Core Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

Up to 6th Gen Intel® Core™ m7 processor
Intel Inside®. Extraordinary Performance Outside
Order here: consumer.huawei.com