Delivering security

Silicon Labs' CSO, **Sharon Hagi**, talks to Neil Tyler about security and product development

The new CSO at Silicon Labs, Sharon Hagi, has responsibility for overseeing the company's cybersecurity strategies and having worked as VP of Security at Ethoca and as Chief Technology Strategist at IBM Security, he has a wealth of experience when it comes to the development of security solutions.

Hagi started his career in embedded software development and moved into security after a start-up he worked for - Secure Computing - was acquired by McAfee, where he was then involved with an innovative firewall project.

Hagi's approach to security comes from a quantitative perspective, as opposed to a qualitative one, which he developed while addressing financial risk management in the financial services industry.

"A lot of risk assessment tends to give things a granular rating which is often based on biases and people's feelings, which can be notoriously inaccurate. I'm a big proponent of leveraging quantitative risk assessment techniques, such as Open FAIR, where you take some of the concepts used for many years in financial risk management and apply them to operational and cybersecurity risk mitigation programs."

In the 1990s financial institutions were seen as pioneers in understanding and reducing risk, today we are facing the same issues with the Internet of Things. Why?

"While we are dealing with a different group of stakeholders, the subject matter is still much the same. The early e-commerce platforms didn't have a consistent set of requirements, so everybody was doing their own thing. Because of time-to-market pressures many chose to do the bare minimum," Hagi suggests.

"It's only when the industry rallied around the issue and made a standard and imposed consequences for non-compliance that e-commerce started to flourish."

According to Hagi, without standards and the pressure financial institutions and the payment processors were putting on the merchants, e-commerce wouldn't have developed in the way it has.

"Today, organisations developing solutions for the IoT space don't have that imperative. While people are looking for all kinds of different regulatory frameworks, we're not seeing consistent treatment from vendors to actually secure those environments," he argues.

Hagi, however, believes that things are changing for the better.

"Everybody acknowledges the importance of security but, for many, the issue is not knowing where to start, or what's sufficient."

According to Hagi, "Standards and regulations are needed to lay down the foundations of what is minimally acceptable and there needs to be a rigorous application of risk management.

"When you're developing a product, companies should sit down with security professionals and figure out what the risk model and possible threats are. In what ways could that system be attacked and what sort of things should you be doing, in terms of security, to prevent that from happening?

"That's the kind of activity that I think the industry has to get behind in order to be more effective in terms of delivering security."

Security and product development

While he's not calling for a revolution, Hagi believes that the industry needs to inject security activities into the product development process.

"At Silicon Labs we are starting to make product features available for our customers to help develop security around their products.

"But there is another issue. Do they actually know how to take advantage of all of this stuff that we're putting in hardware, the software stacks and the gateways to develop compelling applications that have security infused at the right level?"

Hagi says he is looking to address this as part of his new role at Silicon Labs.

"I'm looking at how we are structuring our product strategy and how we help customers address these challenges.

"Customers need to understand security at the very early stages of the product design process. How do we then transition that into engineering, product testing and operational requirements where the product and security is continuously updated to reflect the rapidly evolving threat landscape?

"I hope I'm able to bring a different perspective and a new set of skills to this role, as we look to take security to the next level."

One of the biggest challenges for businesses is how they connect thousands of IoT products to existing security infrastructures.

"Do we need entirely new systems to monitor and manage IoT risk? Or should we build products that are intrinsically able to integrate effectively into existing monitoring management and incident response capabilities," asks Hagi.

"We're talking about things like root of trust and the ability to store keys securely. When you're looking at applications you can code them in such a way that they function basically with the software-only mechanisms. That's what companies and manufacturers have been doing.

"In order to take advantage of hardware features you have to consciously create implementations that call on specific APIs and SDKs to function in certain ways. They are built in ways that are taking advantage and delegating things like encryption and authentication and key generation and all that through those hardware layers."

Securing manufacturing processes is also critical, according to

Hagi.

"After the chip or product leaves the factory, the opportunities to achieve high assurance bootstrapping of identities diminishes. They're still possible, but you don't have that high security opportunity to do that and it's going to cost more to actually bootstrap an identity. The lowest cost opportunity to bootstrap an identity is to be as close as possible to the foundry and we're looking at this as well.

"Silicon manufacturers bootstrap things like silicon identities and that gives you trust in a specific chip. You then have to give access to customers, so that they can leverage those hardware-grounded identities to authenticate against a set of cloud-deployed services and applications and gateways and networks using their issued credentials." According to Hagi, the manufacturing processes involved in getting a chip from a wafer to it being packaged into a SOC, for example, involves very careful orchestration.

"You're introducing delays, so you have to make sure that you are able to inject secrets into those devices, into the chip and the die as well as into the device in aggregate without impacting your costs too much."

Once the device is deployed then you bring in elements of monitoring and threat intelligence and correlation of activities that the IoT device can measure and report on, explains Hagi.

"Is the device being subjected to some kind of an anomalous activity which is an indication of an attack and if it is an attack, what do we do about it? What are the response options? How do we orchestrate that?"

Hagi believes that attacks are likely to affect fleets of devices, so how do you coordinate a response across a relatively large number of connected devices?

"This is a challenge that we haven't really been facing because security, so far, has been about a threat actor attacking a server or attacking a singular target. It has been very rare to see attacks that in aggregate impact a large number of devices all at once," Hagi explains, "and in IoT, that prospect is real and we have to figure out what to do about it."

Hagi argues that companies need to build mechanisms so that devices can actually receive updates securely and from a trusted source and be able to enact on that.

"It's also about, perhaps, identifying a signature of an attack and then updating the device to recognise locally that signature and rejecting a connection attempt or being able to cope with it until, if you will, a more established fix or patch is available. Basically, you need to be able to respond right away."

Companies need to understand the whole process behind incident response orchestration and coordination, argues Hagi.

"The IoT is becoming more automated, with the development of microservices architectures and agile infrastructure where code is being updated on a minute-by-minute basis.

"We have to create IoT devices agile enough to be updated on that frequency. It's a very difficult challenge when you're thinking about highly constrained devices and mesh networks that don't have a lot of battery power."

Silicon Labs has recognised that the IoT will not flourish without security. It is now a real priority and it requires organisational focus and direction.

"That was really the mission that they put in front of me," said Hagi. "We have to make sure that we not only build the most secure products on the market, but we also enable our customers to leverage our capabilities within the hardware and software stacks to build secure solutions."

Security requires a high degree of coordination and collaboration, according to Hagi. "I'm hoping the industry will collaborate to get us to that level where we can buy, as consumers, an IoT product and be confident that it's secure."