A new formula for IoT security is risk equals probability multiplied by loss

The climate of fear surrounding IoT security suggests that it is different to standard IT or internet security but in reality, the fundamentals of securing things are no different to securing servers or personal data. What is different, though, finds George Malim is that in IoT the stakes in terms of the potential damage security breaches can cause are often raised

IoT encompasses such a wide variety of systems, devices, hardware and software that it's daunting to secure and the attack surface is far wider. However, does that really make it different to standard cybersecurity? "IoT security is different because connected devices are primarily embedded, dedicated computer systems and are therefore quite limited," says Kevin Curran, a senior member of the **IEEE** and professor of Cyber Security at the **University of Ulster**. "They are often single purpose devices, performing specific functions within a wider, more complex system – for example, light bulbs, TVs, pacemakers and kettles. IoT security mechanisms should be equally specialised and prevent targeted attacks, which are often unique to device function. Unfortunately, because they are so simplistic, the adoption of security support ecosystems, such as large databases of malware signatures, is impractical. The solution is to enforce rules-based filtering to allow communication only from authorised devices. Firewall policies like this allow a reduced rules set to be adopted."

"The IoT is growing at a rate that is almost unimaginable," confirms Michael Marriott, a research analyst at Digital Shadows

Others see less pronounced differences, although they recognise IoT has specific challenges. "There is no difference between a human digital identity and an IoT identity," says Giovanni Verhaeghe, the director of corporate strategy at **VASCO Data Security**. "The security of IoT identities should be treated with the same level of earnest commitment as they are for human digital identities. However, due to the lack of standardisation in IoT, it is much more complex to create a security strategy."

Jim Sherwood, the head of product liability and a partner at law firm **BLM**, sees elevated security risks associated with the nature of IoT devices and applications. "Increased interconnectivity and the rise of IoT provides a variety of sectors with the opportunity to become more efficient, offer better value to clients or customers and ease day-to-day operations," he says. "Yet with these benefits come complex risks that require stringent security policies. As with regular IT security, there is the potential for significant data leaks; as we saw with the likes of the Ashley Madison and Yahoo! attacks, these can significantly dent consumer trust. With IoT, hackers could have access to multiple devices simultaneously, ultimately escalating data breaches to a scale not yet seen."

Cesare Garlati, the chief security strategist for the **prpl Foundation**, sees the same issue, pointing out that both the threat model and the viable security controls available in IoT are different to other sectors. "The levels of security for both IoT and regular IT security must be robust, regardless, but the consequences if an IoT device was infiltrated could be catastrophic," he says. "With billions of IoT devices now being connected to the physical world, the costs could be life threatening should a device be compromised; and we have already seen the warning signs."

With the increasingly large volumes of IoT deployments, the warning signs are becoming more obvious. "The IoT is growing at a rate that is almost unimaginable," confirms Michael Marriott, a research analyst at **Digital Shadows**. "As a result of this growth, the rapid and successive adoption of newly introduced technologies in the consumer and commercial realms will continue to grow. Furthermore, people will seek to harvest data from these devices and platforms for a variety of reasons, most of which are benign and seek to enhance the overall experience with the technology in question. However, as these new technologies come online the propensity for data to be leaked due to misconfiguration, default insecurity, and/or inherently insecure designs will increase. These security weaknesses can also place those who use and subscribe to the services offered by these devices and platforms at risk."

Such risks are taken seriously but few think the prospect of complete security that is never breached is a likely outcome. Instead organisations will have to continuously battle to ensure they have the most up to date technology and processes in place so they can demonstrate they

are protecting their customers, partners and employees from attacks.

"IoT Security is not a one-off project," says Matthew Dunkley, the IoT strategy director at **Flexera Software**. "IoT companies need to make a continuous effort to protect software and devices, to prevent revenue leakage from accidental overuse and reduce the business risk of reputational damage, data loss, hacking and piracy. To that point, IoT producers have to orchestrate a variety of security and IP protection solutions."

For Sherwood, adopting best practice is a way to demonstrate commitment to addressing security liabilities. "Organisations need to be up-to-date on where liability lies within a complex supply chain of device manufacturers, software developers and service providers," he says. "Data retrieval is challenging, but with any internet-connected device, information sharing is the norm; it needs to be utilised by device manufacturers, or the employees using them, to report vulnerabilities and prevent future attacks. In the event of a breach, companies should be seen to be investigating the incident properly, to begin repairing reputational damage and rebuilding trust. It will be crucial for the board to commit to a thorough and prompt post-breach investigation, implementing appropriate, preventative measures where necessary. Open and honest communication regarding investigations that may affect customers will also be key."

Yet liability is bound to attach itself to organisations so is there a means to balance the risk between the security level required and the risk of attack?

Some industry insiders think there is a formula that can be applied. "Yes [there's a formula:] risk = probability x loss," says Chris Spain, the vice president of cloud solutions at **Cradlepoint**. "Loss can be monetary or reputational and this is a constant battle and the answer will depend on the device type and position. For example, CCTV monitoring in a bank versus CCTV monitoring a scenic view. With non-connected devices one can be compromised at any time. If they are connected when one sneezes it is possible they can all catch the cold with a typical topology centric networking approach. Many of these devices are not upgradeable or patchable and provide a large attack surface."

Emily Ratliff, the head of Security at **Canonical** also thinks formulas can be applied. "Indeed, there are many well documented formulas and models for risk management which can be found in textbooks," she says. "Taking a widely documented one as an example, 'Enterprise Security Architecture: A Business Driven Approach', states: Value at Risk = Value of Potential Loss x Probability of Event x Probability of Failure of Controls. There are organisations which use this and similar formulas with both qualitative and quantitative metrics to calculate total and residual risk. These are primarily banks and other large organisations which can afford the overhead to calculate the numbers and come up with reasonable – agreed-upon – values for the variables."

"For example, for an IoT device, is the asset value $99 per camera device or is the asset value some portion of the market capitalisation of the company which would include reputational impact?" she adds. "Alternatively is it viewed from the consumer perspective of the incalculable cost of embarrassment if the camera catches and leaks a picture that it shouldn't? Documenting the controls – security measures – and performing a gap analysis on the controls is a necessary first step for performing these calculations, but many, maybe most, companies don't seem to perform this security control gap analysis."

For Andrew Till, the vice president technology for partnerships and new solutions at **HARMAN Connected Services**, balancing security with investment is always a decision that each individual company will need to make based on its own unique situation and commercial offerings. "A good first step for any company is conducting a full risk assessment so that it can begin to understand the level of exposure and threats to its business," he says. "This will then help with developing the right balance to ensure sufficient protection but not at excessive costs."

Giovanni Verhaeghe, VASCO Data Security

Michael Marriott, Digital Shadows

Andrew Till, HARMAN Connected Services