Data security and governance in Emerging technologies and IoT - too good to be true?

The IoT trend is transforming virtually every aspect of our lives for the better but connecting the ever-growing number of devices creates additional risks to enterprises and consumers. James Clapper, the U.S. Director of National Intelligence, warned of the risks of the IoT to data privacy, data integrity, or continuity of service in a report presented to the Senate Armed Services Committee that stated, "devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US government systems."

Consumers are right to be concerned about guarding their privacy. When an organization like a hospital connects a new MRI machine to its network, it creates a new cyberattack vector that hackers can use to access or steal data, and even gain control of the hardware itself.

The Identity Theft Resources Center (ITRC) recorded 1,293 breaches last year - 21% higher than 2016 (the previous record-holder). It seemed like a massive data breach made headlines every week last year. So, it's understandable that expectations are high among government regulators and consumers that IoT device manufacturers, and the enterprises that deploy those devices, become better at securing confidential information. But that does not translate to a requirement that companies thwart 100 percent of all cyberattacks.

Consider the EU's General Data Protection Regulation (GDPR), which takes effect May 25. It establishes very strict requirements for protecting customer data, and a tight 72-hour timeframe for reporting a data breach. But if a company can demonstrate it has taken adequate steps to protect information, and promptly notifies affected customers about a breach, it won't be fined for falling victim to the attack.

What regulators and consumers do want to see from manufacturers and organizations that implement connected devices are the highest levels of transparency, responsibility and accountability.
We saw the negative effects of a lack of transparency with the recent discovery of the Spectre and Meltdown vulnerabilities. U.S. lawmakers demanded that representatives from several technology companies explain why they waited months after discovering the vulnerabilities to make the details public. In other words, explain their lack of transparency.

These companies have explained that they were taking time to assess the risk. They were concerned that premature disclosure would have given attackers time to exploit the vulnerabilities. That may be a valid argument, but the damage to their reputations was done.

Effective IoT device security does not mean creating a perfect product that never has any vulnerabilities; it means allowing for a process that addresses quickly and completely all vulnerabilities. An organization must know that when a device is registered and attached to its network that it's legitimate and not fraudulent. Did the device use strong authentication and is

there cryptographic proof that it hasn't been tampered with? Knowing the answer to that question will enable the organization to provide, in a reasonable time frame, complete transparency to auditors and users if a problem arises.

Device authentication can be made easier if open standards are leveraged and incorporated into design phases. Failure to do so inevitably forces them to retrofit devices after-the-fact, an expensive, time-consuming and ineffective approach.

Hardware developers therefore must strike a balance between prioritizing security without diminishing the user experience. Leveraging Public Key Infrastructure (PKI) and digital certificates can be used to meet these requirements. For decades, digital certificates have been the security backbone of networked devices like servers, routers, printers, and fax machines. PKI can do the same for the Internet of Things.

Full transparency provides the public with confidence because there is insight into the company, devices, processes, etc., and demonstrates the company is acting responsibly. Nurturing that perception also requires acknowledging that the IoT landscape is immature. There are so many standards to choose from, and so many different manufacturers, application developers and operating systems. That is why cultivating relationships with the security researcher community matters. Inviting these groups to help identify and report vulnerabilities will enable a manufacturer to more quickly mitigate potential problems. Google recently launched a new bug bounty initiative that demonstrates just how effective that can be.

The Google Play Security Reward Program pays researchers who help uncover vulnerabilities in third-party apps in its Google Play app store. It's like Google's other bug hunting programs for its Chrome browser and Chrome OS. Google taps into an enormous expert community, and demonstrates it takes full responsibility for the Android apps it offers consumers.

Too often with IoT devices, the onus is on the end user to discover and report issues because the device manufacturer does not take that responsibility. Users expect the opposite, so that should be standard operating procedure. Otherwise, lawsuits and regulatory punishments will compel the manufacturer and/or the enterprise that has deployed the devices to do so.

When consumers think of IoT, they likely picture smart home devices like light bulbs they can turn on with voice commands. But enterprises are also embracing IoT. Hospitals use connected devices to improve patient outcomes, the manufacturing sector leverages IoT to create smart environments, such as grids and shop floors where vital information is securely transmitted, captured, and then analyzed in real-time, and IoT serves as the foundations of smart cities nationwide. Automobiles, whether autonomous or human-driven, feature an ever-increasing array of smart sensors, infotainment systems and other components connected to the internet.

All these devices require the highest levels of trust to protect users and the organizations that implement them. Examples such as secure boot, encrypting data at rest and strong device

authentication help gain trust. The security industry can play a lead role in providing the tools to make it easier for manufacturers and organizations make "security by default" a business priority. PKI provides this capability, and certificate authorities (CAs) that are used to operate large-scale PKI systems that adhere to industry standards and requirements can help companies avoid the headache and expense of running their own digital certificate infrastructure. The unique role of PKI in the history of data and identity security, and its ability to facilitate the secure transfer of information across networks, makes it the most effective and ready solution for IoT service providers to demonstrate transparency, responsibility and accountability to their customers, partners and regulators.