SOLUTIONS_

UPDATE TO SINGAPORE CYBERSECURITY ACT ADDRESSES FIRMWARE RISKS

Singapore is one of the most technologically advanced, digitally connected and innovative countries in the world. Whether because of these attributes or simply alongside them, it's also one of the most wealthy countries in the world, with per capita values for GDP (gross domestic product) and GNI (gross national income) that place it consistently in the Top 10 globally according to data from World Bank. The Economics & Commerce Data web site describes Singapore as the fourth largest financial center in the world, the top logistics hub, and the country with the 10th largest foreign reserve.

This success has of course been forged in a world where cybercrime and digital espionage are increasingly commonplace. This has also led Singapore to also be one of the most forward-thinking global leaders when it comes to defining optimal cybersecurity practices. In 2015 the country established the Cyber Security Agency of Singapore (CSA) to keep Singapore's cyberspace safe and secure and to "underpin Singapore's national security, power a digital economy, and protect a digital way of life."

In 2018, the CSA released Singapore's Cyber Security Act of 2018 to provide a legal framework for oversight and maintenance of national cybersecurity throughout Singapore. Designed to constantly evolve through periodic reviews of threat landscapes and adversary activities, the Act looks to address four key objectives:

- Strengthen the protection of critical information infrastructure (CII) against cyberattacks
- Authorize CSA to prevent and respond to cybersecurity threats and incidents
- Establish a framework for sharing cybersecurity information
- Establish a licensing framework for cybersecurity service providers

The Act establishes and regulates cybersecurity best practices through a Cybersecurity Code of Practices for Critical Information Infrastructure, or CoP, document.

After the initial CoP release in in 2018, an update in 2019 inserted "firmware" references in all of its instructions for "patch management" and "malware" defenses, a first indication that the CSA was aware of the sharp increase in firmware-based exploits occurring in the broader threat landscape.

In the most recent version of the CoP, published on July 4 of 2022, an even more significant focus was added for firmware as part of expanded requirements around Secure Coding practices.

REQUIREMENT 10.3.1: FIRMWARE INTEGRITY

The CoP calls out controls for critical information infrastructure (CII) and responsibilities for the managerial owners of that infrastructure (CIIOs). Apart from the CoP's existing definition of firmware as a first-class digital citizen alongside operating systems and applications, this new section of the CoP calls for these owners to focus on security mechanisms and processes for firmware embedded in operational technology (OT) like industrial computers, programmable logic controllers (PLCs) and remote terminal unites (RTUs):

> 10.3.1 The CIIO shall verify the integrity of all embedded firmware of OT CII assets before they are used in the CII, and shall periodically verify the integrity of all embedded firmware in the OT CII.

In addition to this requirement, the CoP calls attention to verification of firmware in field controllers, like the PLCs and RTUs listed above, that are responsible for monitoring and controlling physical access:

> 10.3.2 The CIIO shall verify the integrity of the programme codes in a field controller before use, and shall periodically verify the integrity of all programme codes in field controllers.
>
> 10.3.5 The CIIO shall ensure that no unauthorised changes are made to the programme code or input values of a field controller.

In light of three factors – the relative invisibility of firmware-level code, reticence of many CIIOs to update firmware, and recent firmware-enabled compromises of OT like these on popular Siemens PLCs – many practitioners will find these requirements to be a new challenge.

And they are not alone: a recent report from analyst firm Gartner also highlighted the challenge. Their report called out firmware threat vectors – inclusive of "code injection, tampering and counterfeits" – and then pointed out how the narrowing gap between IT and OT technologies exacerbates existing security problems:

> **It should be noted that the emergence of cyber-physical systems (CPS) – whether born out of the convergence of operational technology and information technology (OT/IT) or born out of Internet of Things (IoT), industrial Internet of Things (IIoT) and Smart X programs (for example, smart cities or smart grids) – further compound the issue.**

ADDITIONAL ZERO TRUST REQUIREMENTS

A new section in the CoP on Design Principles (section 3.5) calls for the use of Zero Trust principles in security design, and while firmware is not explicitly called out, it should be kept in mind as this guidance is followed:

> 3.5.2 The CIIO shall also adopt, to the extent possible… The zero-trust principle to ensure that each request for access to the CII is authenticated, authorised and validated for security configuration and posture before access is granted.

When Zero Trust principles are taken at face value they ask each device to be validated for integrity, as well as all its embedded components. In practice, this means that any endpoint, server, or network device seeking to join the network or transact a session should have it's on-board firmware assessed with an increased level of scrutiny. In essence, all firmware should be continually:

- Identified, so that end use organizations know the detailed source provenance and credibility of the firmware on the device before access is granted to or form the device
- Verified, with that firmware checked against a

known-good baseline, but also for changes made to the underlying firmware that support the device (whether IT or OT)

- Fortified, in the sense that the device should not be allowed access unless its firmware versions are verified as being up-to-date and patched

As mentioned previously, these will be significant tasks for cyber security practitioners who lack visibility and access into their current firmware layers. But the CoP points out a trend – if not outright sounding an alarm – about the need for this level of visibility and access in the future.

NEW CLOUD REQUIREMENTS

An additional revision to the Act's CoP addresses a common practice being undertaken by many organizations: migration of services and systems to cloud environments. While once again not specifically calling out firmware, this language could have significant ramifications when the security posture of firmware is considered:

> 3.7.3 The CIIO shall not implement the whole or any part of the CII on cloud computing systems unless:
>
> (a) It has conducted a cybersecurity risk assessment of the risks relating to and arising from the proposed implementation on cloud computing systems and ensured that the risks identified can be adequately addressed;

The firmware ramification is simply this: in the truest sense, cloud environments are actually instances of an organization's applications and workloads running on "someone else's computer." The attacks we see on firmware are not limited to the firmware beneath an organization's on-prem systems: they exist everywhere.

In 2022 attacks were launched against the baseboard management controllers (BMC) of a popular line of servers, the HP Enterprise Gen8 and Gen9 servers using HPE's iLO4 BMC components. As pointed out by an article in Tech Target, these attacks were specifically engineered to compromise firmware shipped in the BMCs:

> Among the techniques employed by the malware package were fake install screens that would claim to be installing firmware updates in the foreground while actually preventing the install in the background.
>
> The hackers even went so far as update the version number
> on their poisoned firmware to match that of the legitimate iLO version.

Going back to CoP section 3.7.3, CIIOs need to be aware of risk assessments not just in their cloud-based systems, but in the firmware that underlies and supports the hardware driving those systems. Perhaps CIIOs need to begin asking questions of their cloud platform providers like:

- Has firmware in these servers been updated and patched?
- Are there any vulnerable firmware versions to report?
- Can we verify that "our" workloads are running on hardware that has had its firmware reflashed since deployed, and when was that done?

Again, this is likely to be new ground for cyber security practitioners and strategists alike. The vulnerability management and endpoint detection and response solutions currently in use are not built to harvest and report on this kind of firmware-level information. But it may help to know that a new breed of solutions is available to assist.

HOW ECLYPSIUM HELPS

Eclypsium is a firmware security company. Eclypsium's SaaS platform identifies, verifies and fortifies firmware throughout networks and technology supply chains, from endpoints and servers to network gear and connected devices. The Eclypsium platform secures against persistent and stealthy ransomware and malware attacks at the firmware level, provides continuous device and supply chain integrity assessments, delivers firmware patching and updates at scale, and prevents malicious implants.

Details on Eclypsium's firmware security platform can be found here, and a PDF you can share with peers and adjacent teams can be downloaded here. Interested CIIOs are encouraged to contact Eclypsium for product details, breaking threat research, or to speak with a firmware security specialist who knowns and understands Singapore's threat and regulatory landscapes.