

# การเริ่มต้นป้องกันและจัดการภัยไซเบอร์

กฤติยา เอี่ยมศิริ – [krittie@microsoft.com](mailto:krittie@microsoft.com)

Software Asset Management Lead

Microsoft (Thailand) Limited

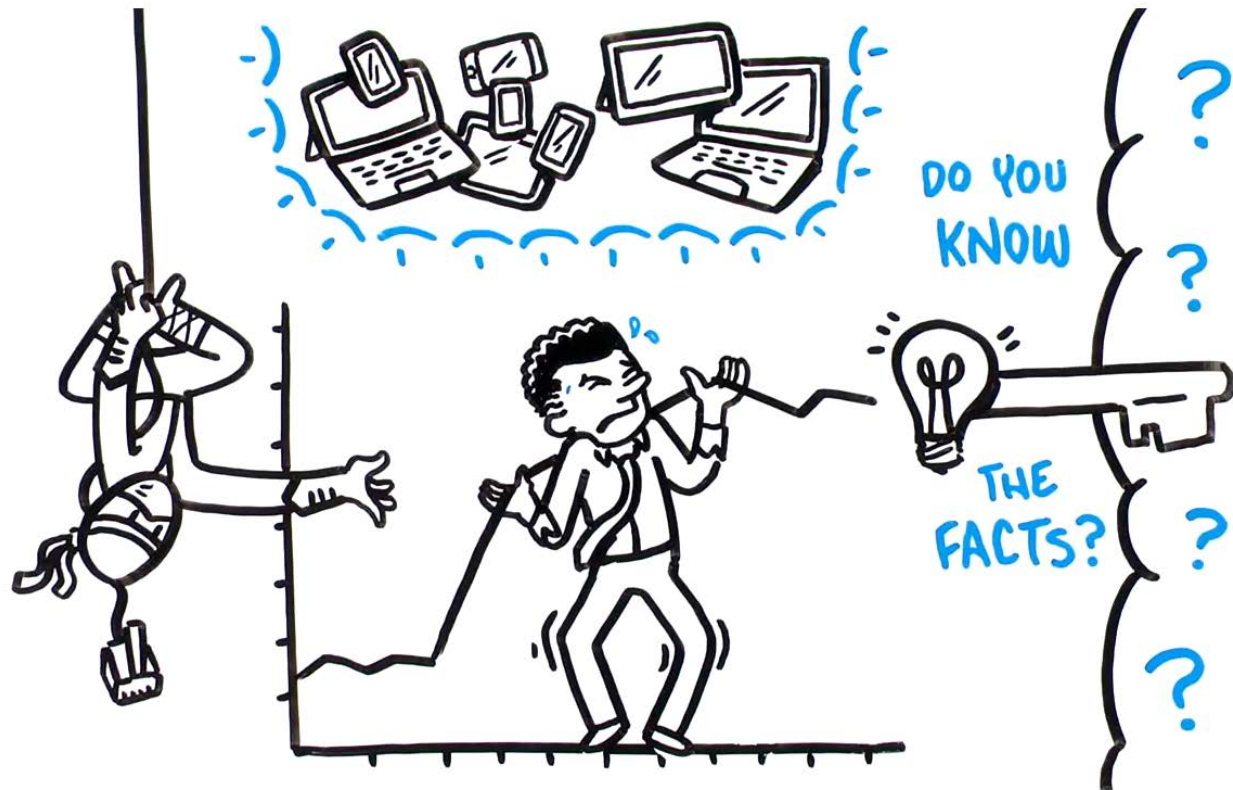




A cluster of five colorful speech bubbles is positioned to the right of the boy. The bubbles are: a red bubble with a white question mark, an orange bubble with the Thai text 'ป้องกัน' (Prevention), a blue bubble with the Thai text 'จัดการ' (Management), a light orange bubble with a white question mark, and a teal bubble with a white question mark.


You cannot Protect what you don't  
know you have got


# สถานการณ์ปัจจุบัน?



# Software Asset Management


## HARDWARE

 = 26,936

 = 548

IOT

 = 7,865

 = 95

AGING  
HW

 = 2,902

 = 31,214  
USERS

DEVICE  
PER  
USER

 = 314

## SOFTWARE

  
WINDOWS  
SERVER

2008 = 516  
2012 = 409

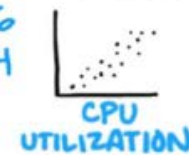
 2010 = 15,957  
2013 = 3,297  
2016 = 48

CLOUD SIZING  
& ACCELERATION

 = 4,918

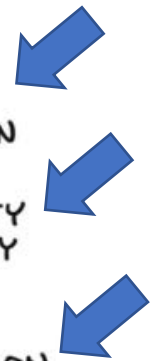
CYBERSECURITY  
& MODERNITY

 2012 = 86  
2016 = 114

  
CPU  
UTILIZATION

  
END OF  
SUPPORT

IT OPTIMIZATION



# SAM for Cybersecurity

---

## CIS CSC20 Ver 7



### Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

### Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

### Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

V7

# Maturity Model pivot for standardization

## Basic

The program is tactical at best and the risks of a Cybersecurity issue, breach, or attack are significant.

## Standardized

The program is proactive and the risks of a Cybersecurity issue, breach, or attack are moderate.

## Rationalized

The program is fully operational and the risks of a Cybersecurity issue, breach or attack are limited.

## Dynamic

The program is strategic and optimal and the risks of a Cybersecurity issue, breach, or attack are minimal.

Details have been created in the SAM Cybersecurity Assessment guidance

Control Domain	Control Domain Description	Basic	Standardized	Rationalized	Dynamic
CSC1	Inventory of Authorized and Unauthorized Devices	No automated asset discovery tool or use of server logging to discover unknown systems (No CSC1 controls and practices in place)	Automated asset discovery tool is used to build a preliminary asset inventory of systems connected to the organization's networks. Use of DHCP server logging to augment asset discovery tools. (CSC1-1, CSC1-2)	Ensures all equipment acquisitions automatically update the inventory system as new devices are connected to the network. Inventory system records at least network addresses, machine names, and ownership. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store and process data are identified. (CSC1-3, CSC1-4)	Deployed network level authentication (e.g., 802.1x) is tied into the inventory data to determine authorized vs. unauthorized systems. Network Access Control (NAC) is used to monitor authorized systems so if an attack occurs the impact can be remediated by moving the untrusted system to a virtual local area network with minimal access. Client certificates are used to validate and authenticate systems. (CSC1-5, CSC1-6, CSC1-7)
CSC2	Inventory of Authorized and Unauthorized Software	No automated software discovery tool or use of whitelisting approach to what software can be installed and run on assets. (No CSC2 controls and practices in place)	Application whitelisting technology is used that allows only software white listed to be used. Devise a list of authorized software and version that is required of the business for each type of system (e.g., servers, workstations, laptops) and validated using file integrity checking tools. (CSC2-1, CSC2-2)	Performs regular scans for unauthorized software generating alerts as needed. A strict change control process is followed around the installation or change of software including checking for versions. Has deployed software inventory tools that track versions at the OS and application layers. (CSC2-3, CSC2-4)	Software inventory tools are integrated with hardware asset inventory tools for single tracking view. Dangerous file types (e.g., .exe, .zip, .msi) are closely monitored and/or blocked. VMs (or air-gaps) are used to isolate applications that are mission critical but are at a higher risk, and workstations are configured with non-persistent, virtualized operating environments that can be restored quickly. Deploys software that has signed IDs. (CSC2-5, CSC2-6, CSC2-7, CSC2-8, CSC2-9)

# ตัวอย่างการประเมิน

## Cybersecurity Future State and Recommendations

Based on the customer's current state, we recommend the following actions to move the SAM program to a full Standardized state.

● Basic ● Standardized ● Rationalized ● Dynamic

Control Domain	Current State	Future State	Suggested Actions
1. Inventory of Authorized and Unauthorized Devices	●	●	<ul style="list-style-type: none"> <li>Upgrade this area of control. Use automated discovery tool along with desktop management and/or Asset management tool to ensure the integrity of asset inventory over time</li> <li>MDM solution should be used. (already in IT plan)</li> </ul>
2. Inventory of Authorized and Unauthorized Software	●	●	<ul style="list-style-type: none"> <li>Upgrade this area of control. Use automated discovery tool along with desktop management and/or Asset management tool to ensure the integrity of asset inventory over time</li> <li>MDM solution should be used. (already in IT plan)</li> <li>A formal Request fulfillment procedure should be used along with ITSM tool to help keep track of requests for Software. This along with the asset management tool will help give a full picture of the Software currently in-used, which will then allow the Customer to do License Optimization in the future as well.</li> </ul>

### 4. Continuous Vulnerability

#### Findings

- Patch management WSUS, however place for control
- There are Security Firewalls, etc. that carried out on a future threats. VA.
- Request in policy approved requests no reviews for actual requests configurations.
- Remediation process formally stated

stream  
nes,  
has  
ificant  
on,  
e  
tion.  
ilities  
be a  
er  
ng  
d  
, and



# SAM ตามลำดับความสำคัญขององค์กร



Infrastructure Optimization



Server Optimization



Cloud Productivity



SAM for Cybersecurity

# Case Studies



สวัสดีครับ ผมชื่อ นันทวัฒน์ นันทวัฒน์  
ผู้อำนวยการด้านเทคโนโลยีสารสนเทศ  
กลุ่มมิตรผล

ผมได้เรียนรู้ว่า การจัดการสินทรัพย์ซอฟต์แวร์  
เป็นสิ่งสำคัญในการปกป้องข้อมูลทางไซเบอร์  
ในยุคดิจิทัล

“ผลที่ได้จาก Software Asset Management for Cybersecurity ทำให้เราเห็นแผนงานถัดไปได้อย่างชัดเจนว่าต้องพัฒนาในด้านใดเพื่อป้องกันภัยคุกคามทางไซเบอร์ในอนาคต”

คุณสันติ สิริทวีชัย ผู้อำนวยการด้านเทคโนโลยีสารสนเทศ  
กลุ่มมิตรผล