Critical Information Infrastructure Protection

Securing Operational Technology

This is not an ADB material. The views expressed in this document are the views of the author/s and/or their organizations and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy and/or completeness of the material's contents, and accepts no responsibility for any direct or indirect consequence of their use or reliance, whether wholly or partially. Please feel free to contact the authors directly should you have queries.

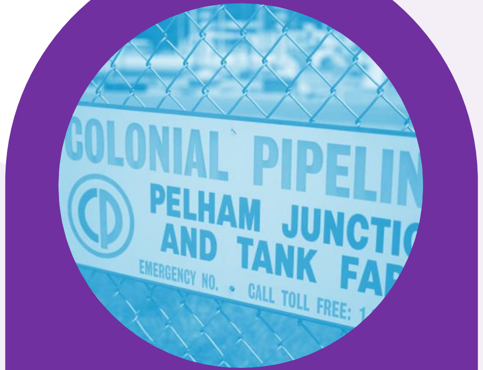
Frits Gerald Enriquez

Incoming Principal, Cybersecurity
KPMG in the Philippines

Cyber Attacks

Osaka hospital hit by ransomware

System outage on its Electronic Medical Record (EMR) system



Ransomware attack forces shutdown of largest fuel pipeline in the U.S.

Hackers breached colonial pipeline using compromised password

Piles of Unpatched IoT, OT Devices Attract ICS Cyberattacks

Industrial devices are less likely to be patched due to expensive downtime, and threat actors have taken notice.

First half of 2023 sees surge in OT & IoT security threats

In the first half of 2023, malware activity in OT and IoT environments worldwide jumped 10x and alerts on unwanted applications doubled as nation-states

Difference of IT and OT

IT

1 **Confidentiality is the top priority**. In order of importance, priorities are: confidentiality, integrity and availability

2 Use of hardware, software and communication systems used to input, store, process and output data

3 The goal is to achieve effective business operations through enterprise solutions, using modern Ethernet and Wireless Protocols.

VS

OT

1 **Control and Availability is the top priority** in OT. In The new order: control, availability, integrity, and confidentiality

2 Use of hardware and software elements to perform real-time monitoring, automation, device control and generate events.

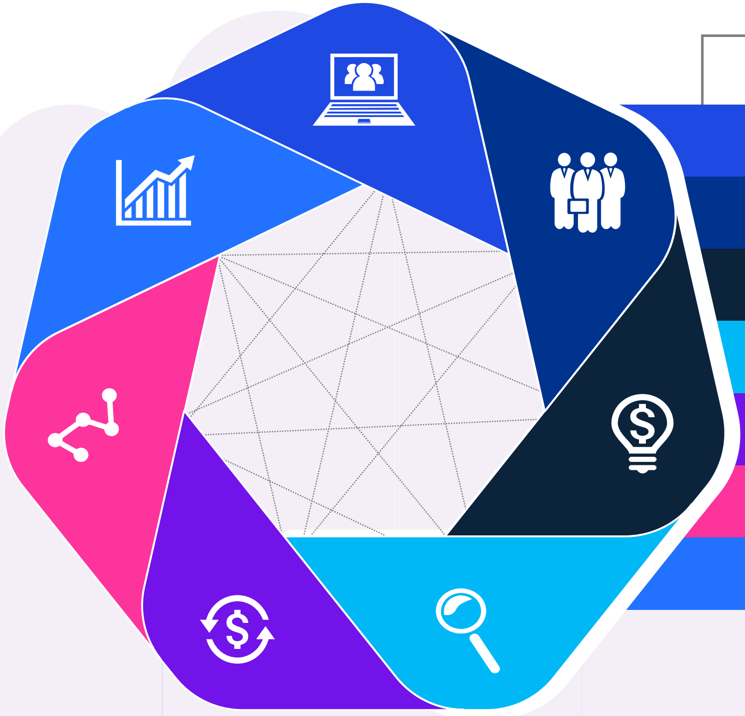
3 The goal is to achieve automation of machines, processes and systems through point-to-point network in isolated environments.

Convergence of IT and OT domains have given rise to shared Cyber Security concerns

- Open-ended access to all devices emerging out of the IT network which allow remote control of OT devices
- Wide range of OT protocols which use cleartext communication that allows eavesdropping
- Advanced threat vectors acting on the OT network causing not only data loss but potentially could harm the human life as well

Drivers to Cybersecurity in OT

Technical



- Digitization: Advent of Smart Grids, AMI
- Disruption in Critical Services
- Digital Twin
- Smart sensors increasing productivity
- Connected Enterprise (Cars, Factories)
- Industry 4.0
- Cyber Security Regulations

Governance

NIST CYBERSECURITY FRAMEWORK
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA
C2M2
Information Security Management System ISO 27001 Certified
IEC
NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
CIS Controls
NATIONAL PRIVACY COMMISSION
ENERGY REGULATORY COMMISSION ERC PHILIPPINES
DICT
GDPR

In the Philippines, The **Critical Information Infrastructure Protection Act of 2022 (CIIPA)** bill establishes a framework for ensuring the security and reliability of the country's digital ecosystem, which is critical to achieving the new administration's goal of safe, seamless, and reliable digitalization and connectivity for all.

Pillars of the National Cybersecurity Plan 2023-2028

Strengthen Cybersecurity Framework

Enhance International Cooperation

Proactively Defend Government Citizens in Cyberspace

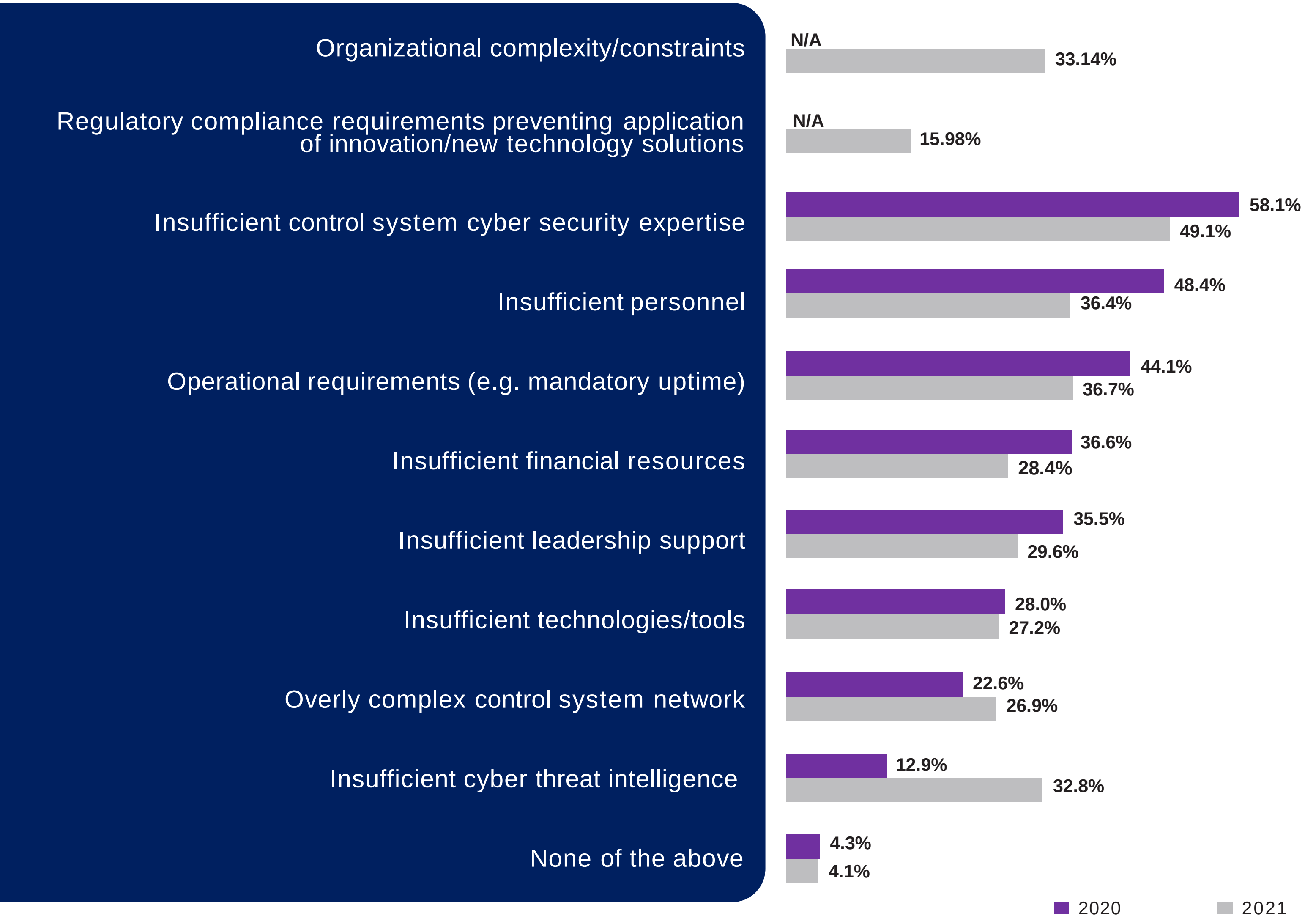
Operational and Well-defined Organization of Nationwide CERT Institutionalized

Increased Capabilities of Workforce in Cybersecurity

Secure and Protect Critical Information Infrastructures

Source: DICT NCSP 2023-2028

Select the greatest obstacles to reducing the control system cyber security attack surface (2020 vs 2021)



Greatest obstacles to reducing the (CS)^2 attack surface

Insufficient control system cyber security expertise continues to be widely considered the greatest obstacle to reducing the control system cyber security attack surface.

In longitudinal analysis, almost all factors received a lower percentage of responses than in our 2020 report, an unsurprising effect of having added two new answer options to this question this year. It is worth noting that *Insufficient Technologies/Tools* was nearly unchanged (27.2 percent this year vs 28.0 percent in 2020) and two others received a larger share of responses.

Insufficient Cyber Threat Intelligence jumped to 32.8 percent (2021) from 12.9 percent (2020) and *Overly Complex Control System Network* rose slightly to 26.9 percent (2021) from 22.6 percent (2020).

Many organizations, of course, do experience frustration from greater administrative complexity and new barriers to network visibility when **implementing greater levels of network segmentation**.

Source: (CS)2 AI — KPMG Control System Cyber Security Annual Report 2022

Technologies in Use

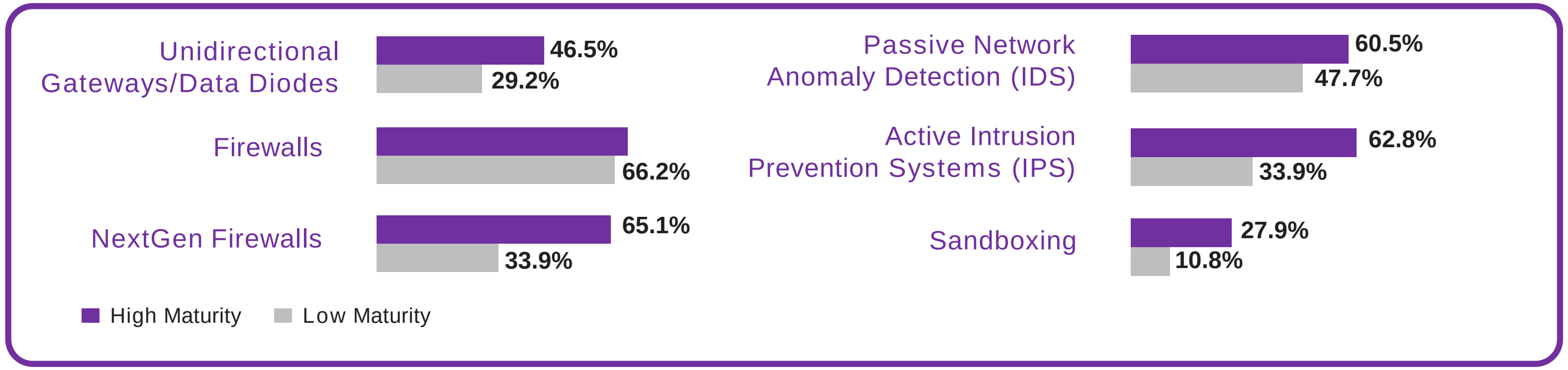
We found several notable trends in security technology use among High Maturity security program organizations. They are roughly half again as likely to use Unidirectional Gateways/Data Diodes (46.5 percent High M vs 29.2 percent Low M), nearly twice as likely to use NextGen Firewalls (65.1 percent High M vs 33.9 percent Low M) and Active Intrusion Prevention Systems (IPS) (62.8 percent High M vs 33.9 percent Low M), and more than twice as likely to use Sandboxing (27.9 percent High M vs 10.8 percent Low M).

Recent Incidents

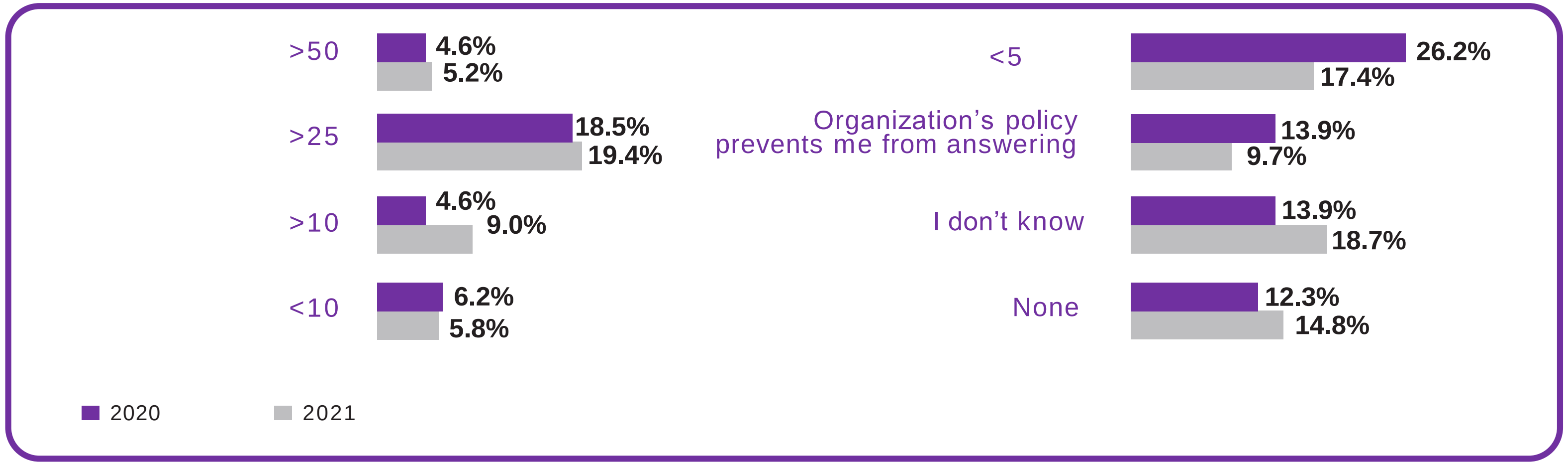
Longitudinal analysis revealed a statistical jump in respondents reporting more than 10 control system cyber security incidents in the past year (4.6 percent in 2020 vs 9.0 percent in 2021) and a drop in reports under five incidents (26.2 percent in 2020 vs 17.4 percent in 2021).

Breaking respondents' organizations into subset by workforce size it quickly becomes clear that their experiences differed. The distinctly higher number of entities in the 500–1,000 employee range reporting more than 25 control system cyber security incidents in the past 12 months (40.9 percent), bracketed by very similar numbers in the 100–500 and 1,000–5,000 ranges (28.6 percent and 28 percent, respectively), along with the sharp drop outside of that range, suggests the possibility that malefactors are targeting companies around this size.

Indicate all security technologies in use to protect your organization's control system assets against cyber threats? (High Maturity vs Low Maturity)



What is your best estimate of how many control system cyber security incidents have occurred in your organization within the past 12 months?



Source: (CS)2 AI — KPMG Control System Cyber Security Annual Report 2022

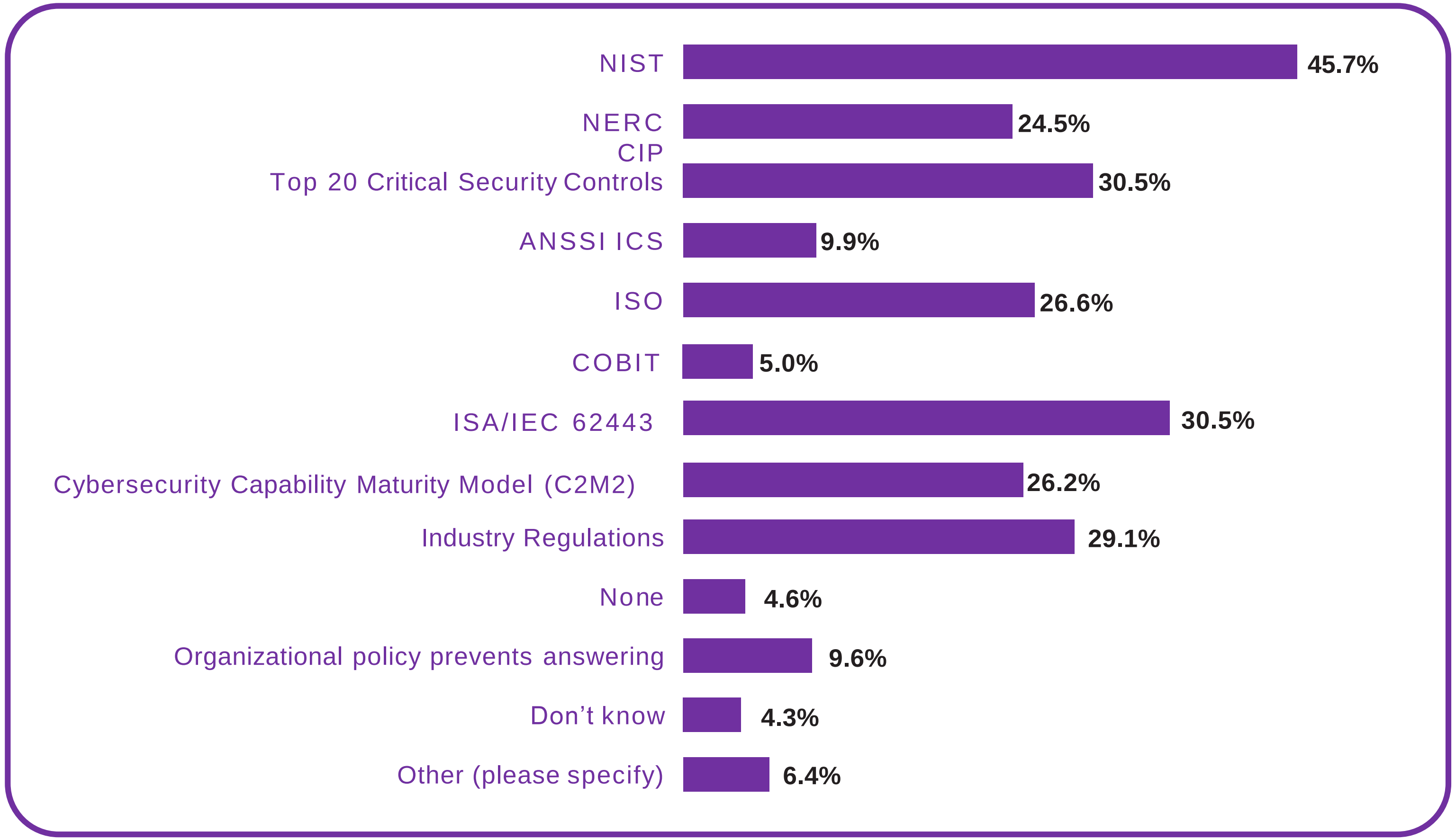
Frameworks in Use

The NIST cyber security framework continues to be the most used. Direct comparison with our previous report is not possible due to changes in this question, but it is worth noting that two answer choices not offered on our original survey, the Cybersecurity Capability Maturity Model (C2M2) and ISA/IEC 62443, are both in widespread use as well (26.2 percent and 36.2 percent, respectively).

The Top 20 Critical Security Controls stood out as the only framework cited more often by respondents with Low Maturity security programs than High Maturity ones (30.1 percent vs 28.6 percent). The High Maturity security program participants reported using every other framework at higher rates, strongly suggesting that their organizations use multiple sources of expertise to guide their programs more often than their counterparts.

The clear takeaway is not that all Low Maturity programs should adopt particular frameworks to improve their security posture, but that these organizations should incorporate more sources of guidance into best practices and processes.

Please select all of the following framework(s) used by your control system security team



Source: (CS)2 AI — KPMG Control System Cyber Security Annual Report 2022

How’s the capacity building?

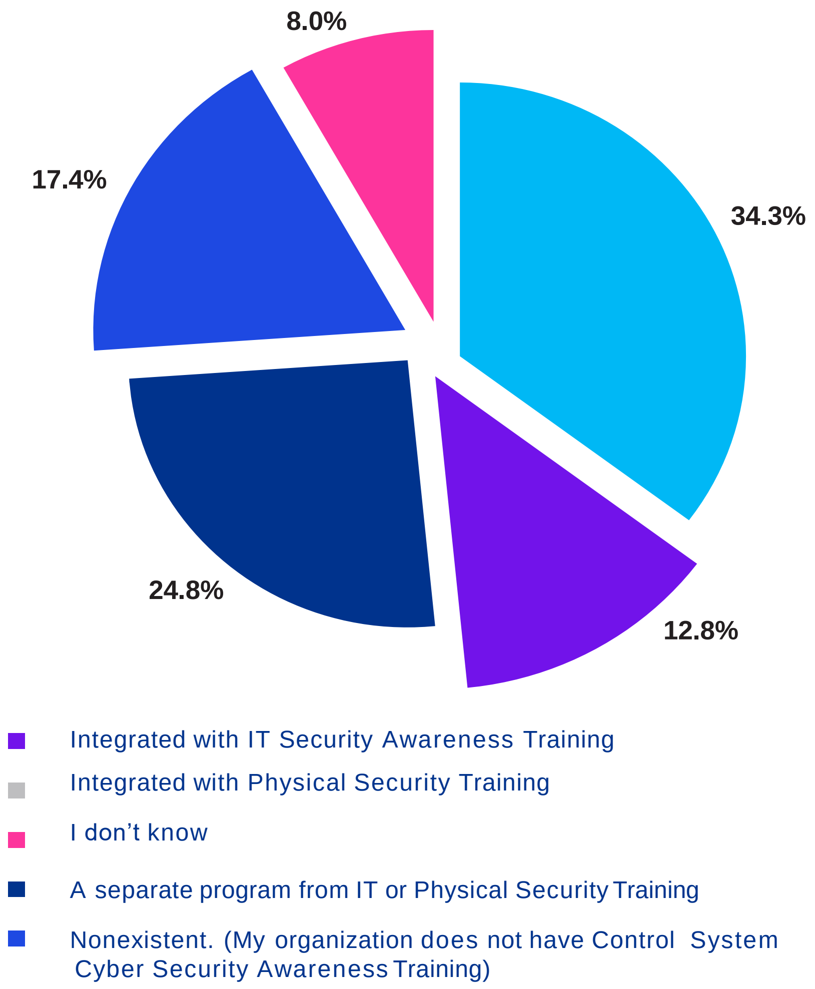
Security awareness training, which aims to improve the security culture of an organization and enable all employees to recognize their role in reducing risk exposures, as opposed to security training which is designed to develop the skills and capabilities of the specialized security practitioners in defending the organization, its assets and resources, is a maturing field in control system settings. Training for IT security awareness and OT safety awareness often have deeper histories of development.

The reasoning and importance of IT security awareness concepts such as validating email sources before clicking unknown links are widely known and understood, for example. Less well understood are the exposures often created when connecting business systems to operational technology, and it is crucial that all organizations address this lack of awareness by delivering control system cyber security awareness training to all their employees, whether they accomplish this by integrating that training with a broader program or as a stand-alone deliverable.

The authors’ key concern is with the over one-sixth (17.4 percent) of respondents whose organizations lack any control system security awareness training at all. While there is a very slight improvement

(20.6 percent in 2020 report), we must stress the importance of educating all personnel regarding their responsibilities in keeping control systems secure

My organization's control system security awareness training is...



Source: (CS)2 AI — KPMG Control System Cyber Security Annual Report 2022

Chief Recommendations

There are a few key concepts underlying our suggested approach to securing your OT environment. Firstly, security is an ongoing pursuit rather than a destination. The ideal state of being completely secure is a hypothetical only and likely not achievable in today's world. Deriving from that, we take as given the core mission of security is to manage risk, i.e., reduce it to acceptable levels. The parameters of this mission are established by organizational leaders, who define risk tolerance and must provide resources needed to bring risks into alignment with that appetite.

The absence of a 'one size-fits all' solution limits the specificity of recommendations to guide those leaders, but we can and do suggest that each organization pursue some basic objectives to the extent possible for them:

Develop your workforce, through **training, education, and creation/improvement of a security culture** within your organization. This will reduce risk of incident occurrence, impacts and recovery time.

Increase your insight into your control system environments by improving **asset inventory and network traffic activity monitoring**. This will reduce the likelihood and duration of disruptions.

Segment your control systems, both from non- operational networks and where feasible, from each other. This will reduce the scope of incidents by limiting their ability to spread.

Investigate your **supply chain security** and implement **controls around entry points into your environments**. This will reduce the potential of attacks on your suppliers impacting you.

Thank you!

Frits Gerald Enriquez

Incoming Principal, Cybersecurity
fmenriquez@kpmg.com
KPMG in the Philippines
(R.G. Manabat & Co.)

Scan to know more about our services

https://home.kpmg/ph/en/home/services/advisory/it-advisory-services.html

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.