The Role of Cybersecurity Community in Supporting National Cyber Space Protection

Rudi Lumanto

idNSA

Key points

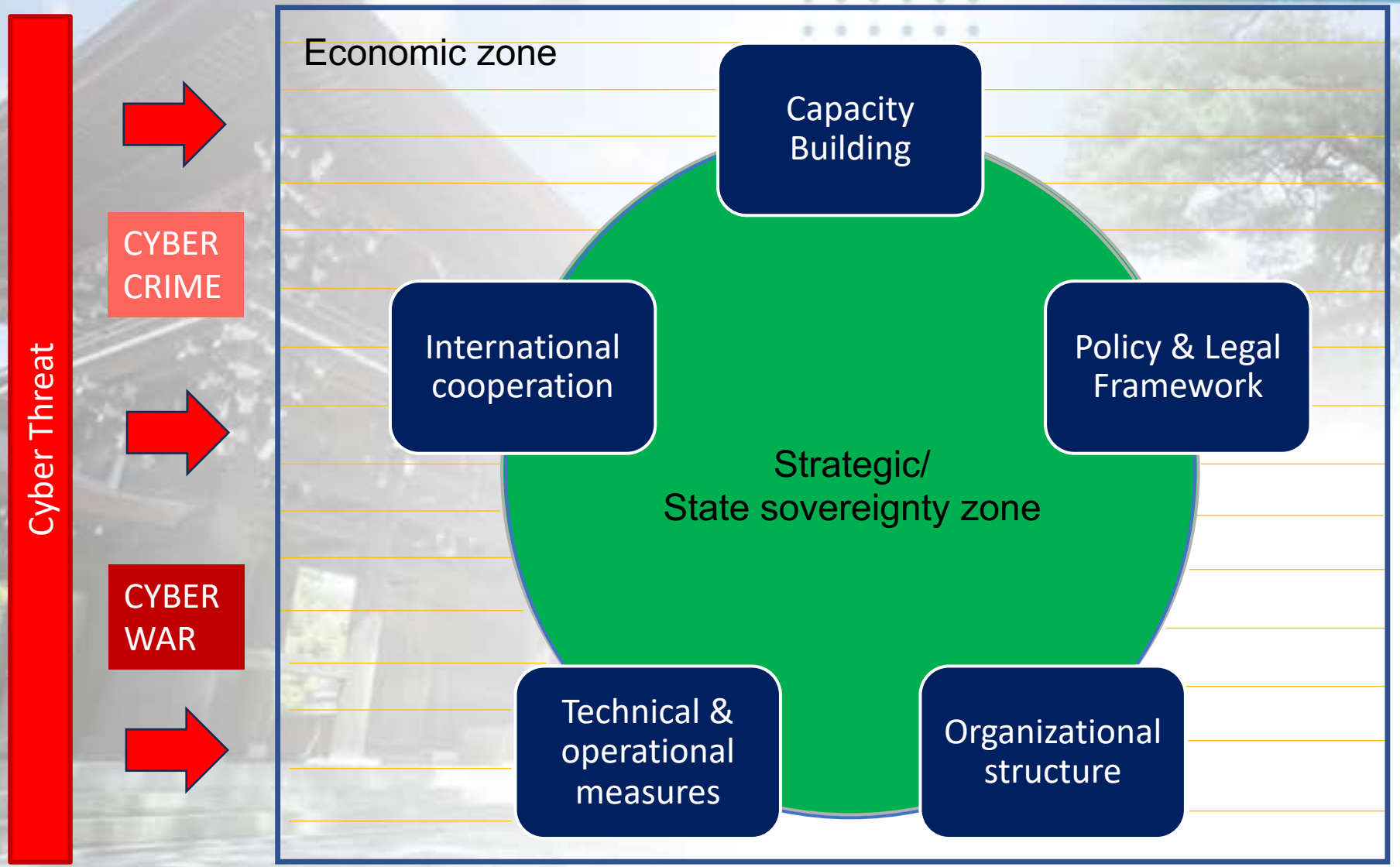
The Role of Cybersecurity Community in Supporting National Cyber Space Protection

National Cyber Space : Cybersecurity in national scale
National Cyber Space protection is whose responsibility ?

The Role of Cybersecurity community ?

50th Year of ASEAN-Japan Friendship and Cooperation

National Cyber Space Protection : Two type of zone protection



Identify

Protect

Detect

Respond

Recover

Cyber Security Awareness

Cyber Hygiene

Cyber Culture

Security Control

50th Year of ASEAN-Japan Friendship and Cooperation

Current Cyber Threats Landscape

- Speed --- rapidly changing threat landscape
- Power --- automate, more complex and sophisticated
- Number – hugh number of threat vectors and attacks

on daily basis, every IP on the internet will get :

- **3000 unsolicited pings**
- **1000 distinct IP address**

(Greynoise)

“Every 14 seconds a ransomware attack targets electrical distribution”

(Schneider Electric)

“A hacker attack happens every 39 seconds”

(University of Maryland)

50th Year of ASEAN-Japan Friendship and Cooperation

Current Cyber Threats Landscape

The biggest threats

1. Phishing Attacks
2. Malware Attacks
3. Ransomware
4. Weak Authentication
5. Insider Threats

Phishing accounts for around 90% of data breaches. grown 65% over the last year, and they account for over $12 billion in business losses.

502 ransomware attacks in July 2023, or more than twice the number of ransomware attacks observed in July 2022. The damages is rising, cost victims $265 billion by 2031

25% of data breach's cause. (verizon)

50th Year of ASEAN-Japan Friendship and Cooperation

World Top Vulnerabilities 2016-2022

2022	2021	2020	2019-2016
CVE-2018-13379	CVE-2021-44228	CVE-2019-19781	CVE-2017-11882
CVE-2021-34473	CVE-2021-40539	CVE-2019-11510	CVE-2017-0199
CVE-2021-31207	CVE-2021-34523	CVE-2018-13379	CVE-2017-5638
CVE-2021-34523	CVE-2021-34473	CVE-2020-5902	CVE-2012-0158
CVE-2021-40539	CVE-2021-31207	CVE-2020-15505	CVE-2019-0604
CVE-2021-26084	CVE-2021-27065	CVE-2017-11882	CVE-2017-0143
CVE-2021- 44228	CVE-2021-26858	CVE-2019-11580	CVE-2018-4878
CVE-2022-22954	CVE-2021-26857	CVE-2018-7600	CVE-2017-8759
CVE-2022-22960	CVE-2021-26855	CVE-2019-0604	CVE-2015-1641
CVE-2022-1388	CVE-2021-26084	CVE-2020-1472	CVE-2018-7600

- Source: The United States Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) report 2020

Top 50 Vulnerabilities distribution is ASEAN Countries in OCT 2022

Rank	Indonesia	Malaysia	Vietnam	Thailand	Singapore	Philippine	Myanmar	Laos	Cambodia	Brunei
1	CVE-2022-28330	CVE-2022-28330	CVE-2022-32548	CVE-2022-28330	CVE-2017-15906	CVE-2022-28330	CVE-2022-28330	CVE-2022-28330	CVE-2022-28330	CVE-2022-28330
2	CVE-2022-28614	CVE-2022-28614	CVE-2018-20012	CVE-2022-28614	CVE-2018-1312	CVE-2022-28614	CVE-2022-28614	CVE-2022-28614	CVE-2022-28614	CVE-2022-28614
3	CVE-2022-28615	CVE-2022-28615	CVE-2021-36368	CVE-2022-28615	CVE-2018-15919	CVE-2022-28615	CVE-2022-28615	CVE-2022-28615	CVE-2022-28615	CVE-2022-28615
4	CVE-2022-29404	CVE-2022-29404	CVE-2020-15778	CVE-2022-29404	CVE-2017-15715	CVE-2022-29404	CVE-2022-29404	CVE-2022-29404	CVE-2022-29404	CVE-2022-29404
5	CVE-2022-30556	CVE-2022-30556	CVE-2017-15906	CVE-2022-30556	CVE-2018-1283	CVE-2022-30556	CVE-2022-30556	CVE-2022-30556	CVE-2022-30556	CVE-2022-30556
6	CVE-2022-31813	CVE-2022-31813	CVE-2018-15473	CVE-2022-31813	CVE-2017-15710	CVE-2022-31813	CVE-2022-31813	CVE-2022-31813	CVE-2022-31813	CVE-2022-31813
7	CVE-2022-22719	CVE-2022-22719	CVE-2018-20685	CVE-2022-22719	CVE-2018-17199	CVE-2022-22719	CVE-2022-22719	CVE-2022-22719	CVE-2022-22719	CVE-2022-22719
8	CVE-2022-22720	CVE-2022-22720	CVE-2019-6109	CVE-2022-22720	CVE-2019-0220	CVE-2022-22720	CVE-2022-22720	CVE-2022-22720	CVE-2022-22720	CVE-2022-22720
9	CVE-2022-22721	CVE-2022-22721	CVE-2019-6110	CVE-2022-22721	CVE-2017-7679	CVE-2022-22721	CVE-2022-22721	CVE-2022-22721	CVE-2022-22721	CVE-2022-22721
10	CVE-2021-44790	CVE-2021-44790	CVE-2019-6111	CVE-2021-44790	CVE-2016-8612	CVE-2021-44790	CVE-2021-44790	CVE-2021-44790	CVE-2021-44790	CVE-2021-44790
11	CVE-2021-34798	CVE-2021-34798	CVE-2020-14145	CVE-2021-34798	CVE-2017-9798	CVE-2021-34798	CVE-2021-34798	CVE-2021-34798	CVE-2021-34798	CVE-2021-34798
12	CVE-2021-39275	CVE-2021-39275	CVE-2021-41617	CVE-2021-39275	CVE-2016-4975	CVE-2021-39275	CVE-2021-39275	CVE-2021-39275	CVE-2021-39275	CVE-2021-39275
13	CVE-2021-40438	CVE-2021-40438	CVE-2018-15919	CVE-2021-40438	CVE-2019-0211	CVE-2021-40438	CVE-2021-40438	CVE-2021-40438	CVE-2021-40438	CVE-2021-40438
14	CVE-2022-26377	CVE-2022-26377	CVE-2022-28330	CVE-2022-26377	CVE-2019-0196	CVE-2022-26377	CVE-2022-26377	CVE-2022-26377	CVE-2022-26377	CVE-2018-1301
15	CVE-2022-23943	CVE-2022-23943	CVE-2022-28614	CVE-2022-23943	CVE-2017-9798	CVE-2022-23943	CVE-2022-23943	CVE-2022-23943	CVE-2022-23943	CVE-2018-1302
16	CVE-2020-13938	CVE-2018-1301	CVE-2022-28615	CVE-2020-13938	CVE-2018-1333	CVE-2020-13938	CVE-2019-17567	CVE-2019-17567	CVE-2020-13938	CVE-2018-1303
17	CVE-2020-35452	CVE-2018-1302	CVE-2022-29404	CVE-2020-35452	CVE-2019-0197	CVE-2020-35452	CVE-2020-13938	CVE-2020-13938	CVE-2020-35452	CVE-2017-9798
18	CVE-2021-26690	CVE-2018-1303	CVE-2022-30556	CVE-2021-26690	CVE-2018-11763	CVE-2021-26690	CVE-2020-35452	CVE-2020-35452	CVE-2021-26690	CVE-2017-9788
19	CVE-2021-26691	CVE-2020-13938	CVE-2022-31813	CVE-2021-26691	CVE-2016-8743	CVE-2021-26691	CVE-2021-26690	CVE-2021-26690	CVE-2021-26691	CVE-2016-8612
20	CVE-2019-17567	CVE-2020-35452	CVE-2022-22719	CVE-2019-17567	CVE-2017-3167	CVE-2019-17567	CVE-2021-26691	CVE-2021-26691	CVE-2019-17567	CVE-2017-7679
21	CVE-2020-1927	CVE-2021-26690	CVE-2022-22720	CVE-2020-1927	CVE-2017-3169	CVE-2020-1927	CVE-2020-1927	CVE-2020-1927	CVE-2020-1927	CVE-2017-3167
22	CVE-2020-1934	CVE-2021-26691	CVE-2022-22721	CVE-2020-1934	CVE-2017-7868	CVE-2020-1934	CVE-2020-1934	CVE-2020-1934	CVE-2020-1934	CVE-2016-4975
23	CVE-2021-44224	CVE-2019-17567	CVE-2021-44790	CVE-2018-1301	CVE-2019-9637	CVE-2021-44224	CVE-2021-44224	CVE-2018-1301	CVE-2022-31629	CVE-2016-5387
24	CVE-2019-10098	CVE-2020-1927	CVE-2021-34798	CVE-2018-1302	CVE-2019-9638	CVE-2019-10098	CVE-2021-33193	CVE-2018-1302	CVE-2022-31629	CVE-2016-8743
25	CVE-2019-10092	CVE-2020-1934	CVE-2021-39275	CVE-2018-1303	CVE-2019-9639	CVE-2019-10092	CVE-2019-10098	CVE-2018-1303	CVE-2018-1301	CVE-2015-0228
26	CVE-2019-0220	CVE-2017-9798	CVE-2021-40438	CVE-2021-44224	CVE-2019-9641	CVE-2018-1301	CVE-2019-10092	CVE-2021-44224	CVE-2018-1302	CVE-2015-3183
27	CVE-2019-0217	CVE-2017-9788	CVE-2022-26377	CVE-2019-10098	CVE-2013-6438	CVE-2018-1302	CVE-2020-11993	CVE-2017-9798	CVE-2018-1303	CVE-2014-0231
28	CVE-2018-1301	CVE-2017-7679	CVE-2022-23943	CVE-2019-10092	CVE-2014-0098	CVE-2018-1303	CVE-2020-9490	CVE-2017-9788	CVE-2021-44224	CVE-2013-5704
29	CVE-2018-1302	CVE-2017-3167	CVE-2020-13938	CVE-2019-0220	CVE-2018-19935	CVE-2019-0220	CVE-2019-0220	CVE-2017-7679	CVE-2019-10098	CVE-2014-0118
30	CVE-2018-1303	CVE-2016-8612	CVE-2020-35452	CVE-2019-0217	CVE-2014-0231	CVE-2019-0217	CVE-2019-0217	CVE-2017-3167	CVE-2019-10092	CVE-2014-0226
31	CVE-2021-33193	CVE-2016-8743	CVE-2021-26690	CVE-2017-9798	CVE-2020-1927	CVE-2021-33193	CVE-2018-17199	CVE-2019-10098	CVE-2019-0220	CVE-2013-6438
32	CVE-2018-17199	CVE-2016-5387	CVE-2021-26691	CVE-2017-9788	CVE-2019-9024	CVE-2018-17199	CVE-2018-1301	CVE-2019-10092	CVE-2019-0217	CVE-2014-0098
33	CVE-2022-2068	CVE-2016-4975	CVE-2019-17567	CVE-2018-17199	CVE-2019-9020	CVE-2017-9798	CVE-2018-1302	CVE-2019-0220	CVE-2018-17199	CVE-2017-3735
34	CVE-2022-1292	CVE-2015-0228	CVE-2020-1927	CVE-2017-7679	CVE-2019-9021	CVE-2017-9788	CVE-2018-1303	CVE-2019-0217	CVE-2017-9798	CVE-2022-1292
35	CVE-2022-0778	CVE-2015-3183	CVE-2020-1934	CVE-2017-3167	CVE-2019-9023	CVE-2017-7679	CVE-2018-1312	CVE-2016-4975	CVE-2017-9788	CVE-2022-2068
36	CVE-2018-1312	CVE-2014-0231	CVE-2018-1301	CVE-2021-33193	CVE-2018-17082	CVE-2017-3167	CVE-2017-15710	CVE-2016-8743	CVE-2019-9637	CVE-2022-0778
37	CVE-2017-15715	CVE-2013-5704	CVE-2018-1302	CVE-2016-8612	CVE-2018-14883	CVE-2016-8612	CVE-2017-15715	CVE-2016-5387	CVE-2019-9638	CVE-2017-3169
38	CVE-2017-15710	CVE-2019-10098	CVE-2018-1303	CVE-2016-4975	CVE-2018-15132	CVE-2020-11993	CVE-2018-1283	CVE-2016-8612	CVE-2019-9639	CVE-2019-1552
39	CVE-2018-1283	CVE-2019-10092	CVE-2022-31629	CVE-2016-8743	CVE-2018-20783	CVE-2020-9490	CVE-2021-36160	CVE-2021-33193	CVE-2019-9641	CVE-2021-4160
40	CVE-2021-4160	CVE-2014-0118	CVE-2022-31629	CVE-2016-5387	CVE-2018-1301	CVE-2016-4975	CVE-2017-9798	CVE-2018-20012	CVE-2015-9253	CVE-2019-1547
41	CVE-2017-9798	CVE-2014-0226	CVE-2019-10098	CVE-2018-1312	CVE-2018-1302	CVE-2016-8743	CVE-2020-11984	CVE-2020-15778	CVE-2017-7679	CVE-2019-1563
42	CVE-2017-9788	CVE-2019-0220	CVE-2019-10092	CVE-2017-15715	CVE-2018-1303	CVE-2016-5387	CVE-2017-9788	CVE-2021-36368	CVE-2017-3167	CVE-2018-0734
43	CVE-2017-7679	CVE-2019-0217	CVE-2017-9798	CVE-2017-15710	CVE-2018-19395	CVE-2018-1312	CVE-2017-7679	CVE-2017-15906	CVE-2017-7272	CVE-2021-23840
44	CVE-2017-3167	CVE-2013-6438	CVE-2017-9788	CVE-2018-1283	CVE-2019-6977	CVE-2017-15715	CVE-2017-3167	CVE-2018-15473	CVE-2017-7863	CVE-2021-23841
45	CVE-2021-3712	CVE-2014-0098	CVE-2019-0220	CVE-2022-31628	CVE-2018-19396	CVE-2017-15710	CVE-2016-8612	CVE-2018-20685	CVE-2018-19395	CVE-2020-1971
46	CVE-2022-31628	CVE-2022-31628	CVE-2019-0217	CVE-2022-31629	CVE-2018-10546	CVE-2018-1283	CVE-2016-4975	CVE-2018-17199	CVE-2018-19396	CVE-2021-3712
47	CVE-2022-31629	CVE-2022-31629	CVE-2017-7679	CVE-2022-2068	CVE-2018-10548	CVE-2022-0778	CVE-2016-8743	CVE-2019-6109	CVE-2019-9020	CVE-2018-0732
48	CVE-2016-4975	CVE-2018-17199	CVE-2017-3167	CVE-2015-0228	CVE-2018-10549	CVE-2022-2068	CVE-2016-5387	CVE-2019-6110	CVE-2019-9021	CVE-2017-3736
49	CVE-2016-8743	CVE-2021-44224	CVE-2016-8612	CVE-2015-3183	CVE-2018-10547	CVE-2015-0228	CVE-2022-0778	CVE-2019-6111	CVE-2019-9023	CVE-2017-3738
50	CVE-2016-5387	CVE-2017-15715	CVE-2018-17199	CVE-2022-1292	CVE-2018-10545	CVE-2015-3183	CVE-2022-1292	CVE-2015-0228	CVE-2019-9024	CVE-2019-1551

Year 2022	Year 2021	Year 2020	Year 2019	Year 2018	Year 2017	Year 2016	Year 2015 - 2014 - 2013

ASEAN-Japan
Friendship and Cooperation

Source : idnsa.id

Role of Cybersecurity Community

OWASP: The Open Web Application Security Project (OWASP) is a community-driven organization that focuses on improving the security of software. They provide resources, tools, and guidelines to enhance web application security.

Center for Internet Security (CIS): CIS is a nonprofit organization that works to enhance the cybersecurity readiness and resilience of public and private sector entities. They provide tools, best practices, and resources to improve cybersecurity.

Internet Society (ISOC): ISOC is a nonprofit organization dedicated to promoting an open and secure Internet. They focus on standards development, policy advocacy, and capacity building in cybersecurity.

50th Year of
ASEAN-Japan
Friendship and Cooperation

The Role of Cybersecurity Community

Framework	Role
Identify	Threat Intelligence
Detect	Vulnerability Disclosure, Community Watchdog, Advisory Services, Security Solutions
Protect	Monitoring and Analysis, Threat Hunting
Respond	Advisory Services during incident response efforts and forensic investigation
Recover	Shares lessons learned from incidents

Defense in Depth strategy by all to all

50th Year of ASEAN-Japan Friendship and Cooperation

The Role of Cybersecurity Community

- Promoting cybersecurity awareness
  - no 100% protection
  - you must protect your self
  - empower and strengthen the surrounding

-understanding
- engagement
- commitment

50th Year of ASEAN-Japan Friendship and Cooperation

Key points summary

- The role of communities are very important now but it only as complement to the role of government.
- Strengthening ASEAN Japan relationship not only among government to government but also across the communities in ASEAN and Japan.
- It is not what Japan can do for ASEAN but what Japan can do with ASEAN
- People to people ties are source of strength and we strongly believe that this new collaboration is committed to these ties

50th Year of ASEAN-Japan Friendship and Cooperation