

# "Tingkat Kesadaran Keamanan Siber pada ASN"

Setiadi Yazid

Center for Cyber Security and Cryptography, Universitas Indonesia

# Alur paparan

- Progres dunia siber
- Faktor manusia pada keamanan siber
- Beda ASN dan non ASN
- Pembentukan budaya keamanan siber

JAN  
2021

# DIGITAL AROUND THE WORLD

ESSENTIAL HEADLINES FOR MOBILE, INTERNET, AND SOCIAL MEDIA USE

INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS

TOTAL  
POPULATION



**7.83**  
BILLION

URBANISATION:

**56.4%**



UNIQUE MOBILE  
PHONE USERS



**5.22**  
BILLION

vs. POPULATION:

**66.6%**

we  
are  
social

INTERNET  
USERS\*



**4.66**  
BILLION

vs. POPULATION:

**59.5%**



ACTIVE SOCIAL  
MEDIA USERS\*



**4.20**  
BILLION

vs. POPULATION:

**53.6%**

8

**SOURCES:** THE U.N.; LOCAL GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY EARNINGS REPORTS; MEDIASCOPE. **\*ADVISORIES:** INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** TO DATA PUBLISHED IN PREVIOUS REPORTS. SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES.

we  
are  
social



Hootsuite®

<https://datareportal.com/reports/digital-2021-global-overview-report>

JAN  
2021

# GLOBAL DIGITAL GROWTH

THE YEAR-ON-YEAR CHANGE IN DIGITAL ADOPTION

INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS

TOTAL  
POPULATION



we  
are  
social

**+1.0%**

JAN 2021 vs. JAN 2020

**+81 MILLION**

UNIQUE MOBILE  
PHONE USERS



**+1.8%**

JAN 2021 vs. JAN 2020

**+93 MILLION**

INTERNET  
USERS\*



**+7.3%**

JAN 2021 vs. JAN 2020

**+316 MILLION**

ACTIVE SOCIAL  
MEDIA USERS\*



**+13.2%**

JAN 2021 vs. JAN 2020

**+490 MILLION**

9

**SOURCES:** THE U.N.; LOCAL GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY EARNINGS REPORTS; MEDIASCOPE. **\*ADVISORIES:** INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** TO DATA PUBLISHED IN PREVIOUS REPORTS. SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **◆ COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES.

we  
are  
social



Hootsuite®

# BSSN: Hingga Agustus 2021 Tercatat 888 Juta Serangan Siber

- "Di tahun sampai dengan sekarang Agustus itu hampir 888 juta serangan ya," kata Hinsa dalam acara Pembukaan Program Digital Leadership Academy, Senin (13/9/2021).  
"Yang lebih banyak itu (serangan) malware, denial of service ya mengganggu ketersediaan layanan, trojan activity dan sebagainya," lanjut dia.  
"Serangan kedua adalah bersifat sosial, yang diserang siapa di sini, lapisan ketiga yaitu manusia dengan adanya berita-berita hoaks dan sebagainya," ujarnya.

# Kekhususan dunia siber

## **Dunia Siber**

- Sejak th 1940 an
- Tidak ada hukum alam
- Tidak ada batas geografis
- Bisa dibuat sesuai keinginan
- Tidak ada polisi
- Kecurian X kehilangan

## **Dunia nyata**

- Sejak dunia tercipta
- Hukum alam berlaku
- Ada batas geografis, waktu, dll
- Ada pola yang berlaku
- Ada penegak hokum
- Kebocoran/kecurian = hilang

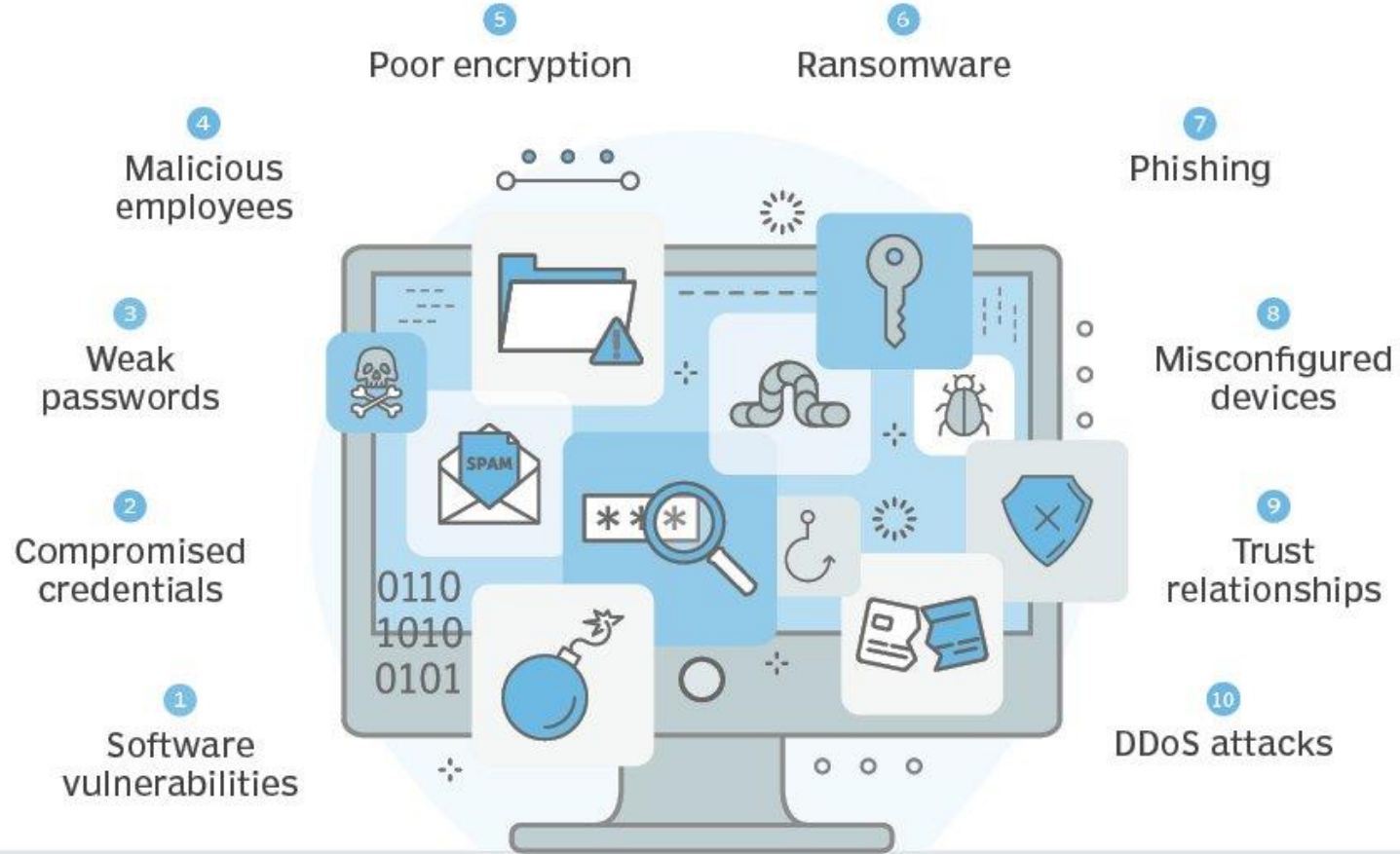
# Most CISOs believe that human error is the biggest risk for their organization

53% of CISOs and CSOs in the UK&I reported that their organization suffered at least one significant cyberattack in 2020, with 14% experiencing multiple attacks, a Proofpoint survey reveals.



- <https://www.helpnetsecurity.com/2021/01/21/cisos-human-error-risk/>

# 10 common attack vectors



### Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

### Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.



### Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

### Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

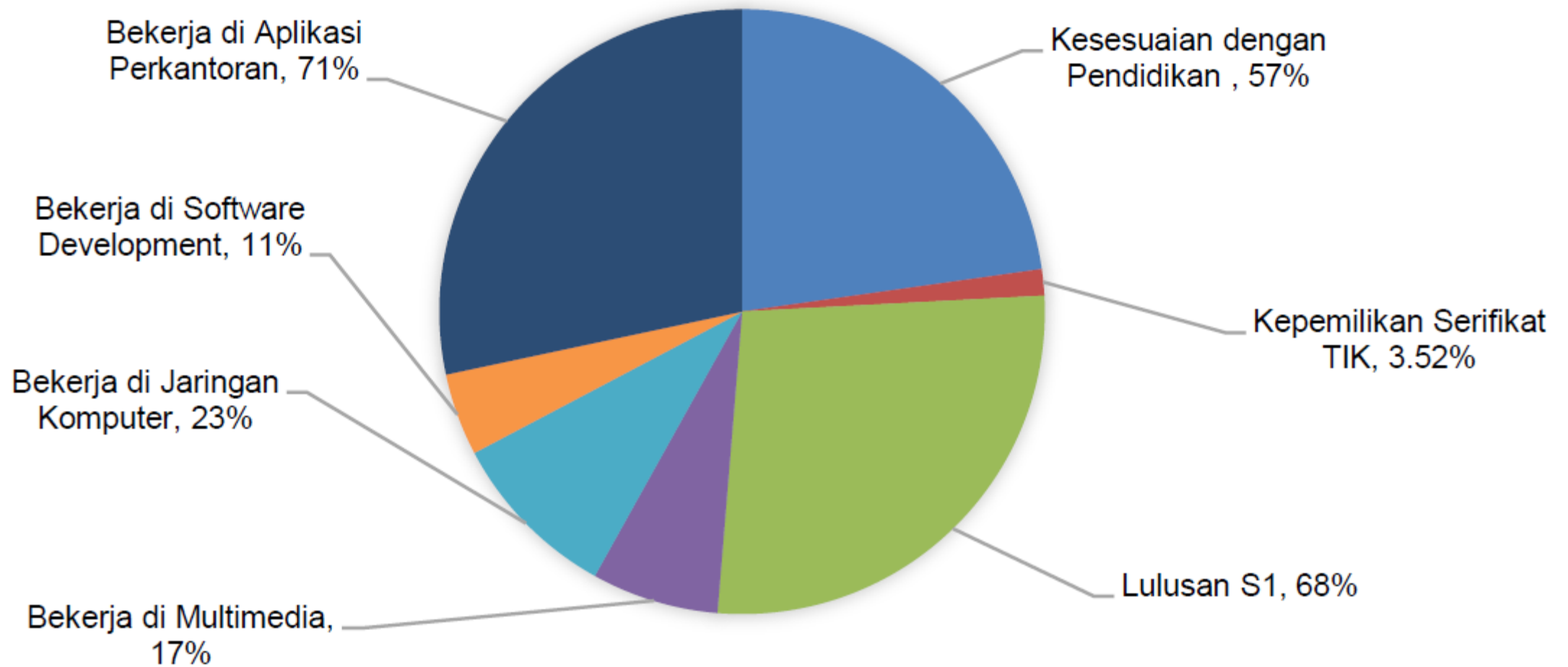
# Mengapa khusus ASN

## **ASN**

- Non profit
- Untuk pemerintah
- Politik
- “Full time”
- Relasi
- Shame culture

## **NON ASN**

- Profit
- Perusahaan
- Finansial
- Full time
- Kemampuan teknis
- Guilt culture



---

**mbar 5.** Bagan Profil dan Pemetaan SDM TIK (Sumber Olahan dari Kementerian Kominfo 2019)

# Keleboboran data eHac

- Meski telah dihubungi sebanyak dua kali, hingga awal Agustus, vpnMentor belum juga menerima respons dari Kemenkes. Menanggapi masalah serius ini, vpnMentor kemudian berupaya menjangkau instansi pemerintahan lainnya seperti BSSN. "Kami menghubungi mereka pada tanggal 22 Agustus dan mereka menjawab pada hari yang sama. Dua hari kemudian, pada 24 Agustus, server dimatikan," tulis pihak vpnMentor.

<https://tekno.tempo.co/read/1501923/kronologi-keleboboran-data-pengguna-aplikasi-ehac-hingga-akhirnya-dinonaktifkan>

- "Kemenkes memastikan bahwa data masyarakat yang ada dalam sistem eHAC tidak bocor dan dalam perlindungan, data masyarakat yang ada di dalam eHAC tidak mengalir ke platform mitra," ungkap Anas dalam konferensi pers Kemenkes RI Rabu (1/9/2021).

<https://health.detik.com/berita-detikhealth/d-5706224/kemenkes-klaim-data-ehac-tidak-bocor-ini-yang-sebenarnya-terjadi>

# BIN Bantah Servernya Diretas Hacker China

- Wawan menjelaskan, selama ini BIN selalu melakukan pengecekan secara berkala terhadap sistem yang berjalan, termasuk server. Hal ini dilakukan untuk memastikan bahwa server tersebut tetap berfungsi sebagaimana mestinya. Ia juga mengatakan, serangan serangan yang mengarah ke BIN merupakan hal wajar.
- Meski demikian, seorang sumber mengatakan kepada Insikt Group bahwa pihak terkait telah menempuh sejumlah langkah untuk mengidentifikasi dan membersihkan sistem yang berhasil dibobol tadi.
- Namun, beberapa hari setelah informasi dari sumber tersebut menyeruak, para peneliti dari Insikt Group meyakini bahwa mereka masih bisa mendeteksi bahwa jaringan internal yang sebelumnya dibobol masih tersambung dengan server Mustang Panda.

# Building a culture of cybersecurity: 3 key takeaways from the 2021 SANS report

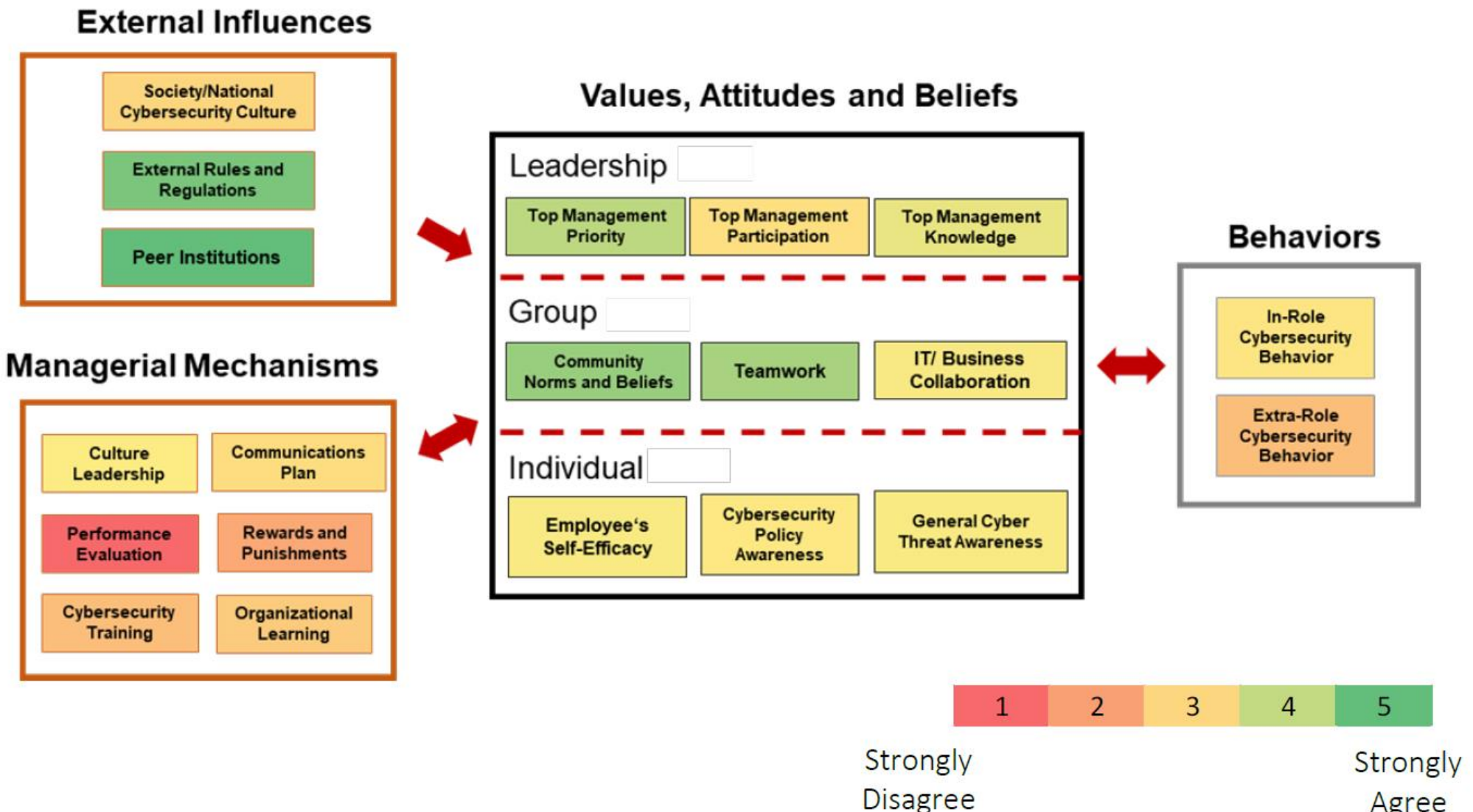
- **Time is the top challenge, not budget:** Almost 75% of security awareness professionals spend less than half of their time on security awareness, indicating that awareness is usually not a full-time effort in most businesses. Organizations that attribute culture change through security awareness are making significant, long-term investments and have more than three full-time, dedicated resources focused on security awareness alone.
- **Awareness program leaders lack soft skills:** Security awareness programs are often led by people with technical prowess but lack adequate communication and marketing skills which can effectively engage employees, influence a change in behavior and have a measurable impact on security culture.
- **Lack of strategic alignment:** Security awareness professionals often lack leadership support or are aligned to teams that are not focused on security exclusively, such as HR, legal, accounting, etc. SANS recommends that security programs should be an extension of the security teams and must report directly to the CISO if possible.

# *16Shop: Commercial Phishing Kit Has A Hidden Backdoor*

- The alleged developer of 16Shop, an Indonesian known only as Riswanda or 'devilscream', has either created a sophisticated false identity, or given up on the notion of protecting their real identity entirely. Akamai researchers, as well as other [researchers online](#), have located various personal artifacts of Riswanda's, including GitHub repositories, security presentations, past examples of website defacements, pictures of family and friends, email address, and social media accounts.*

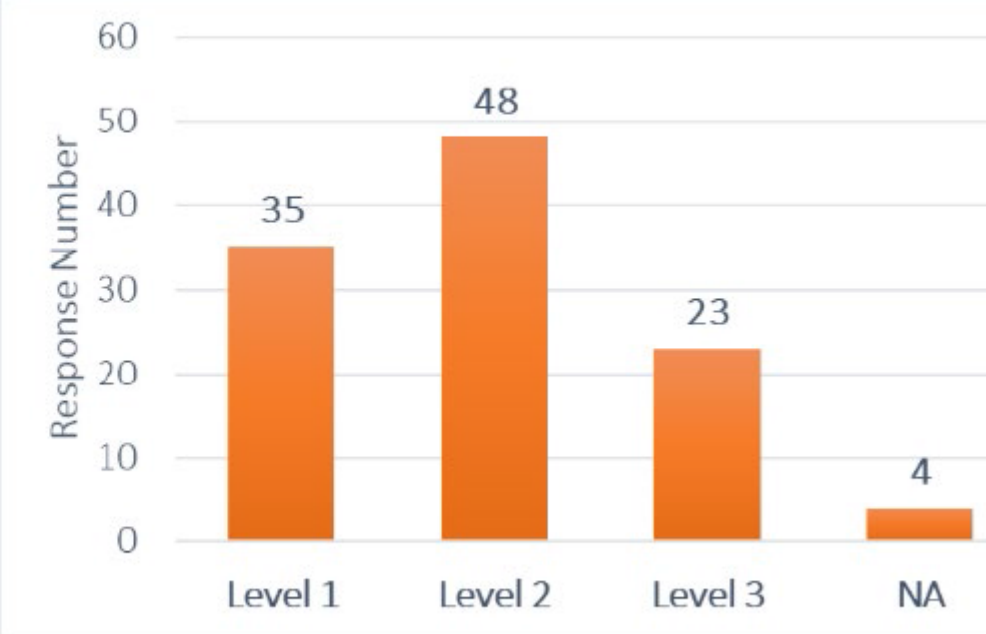
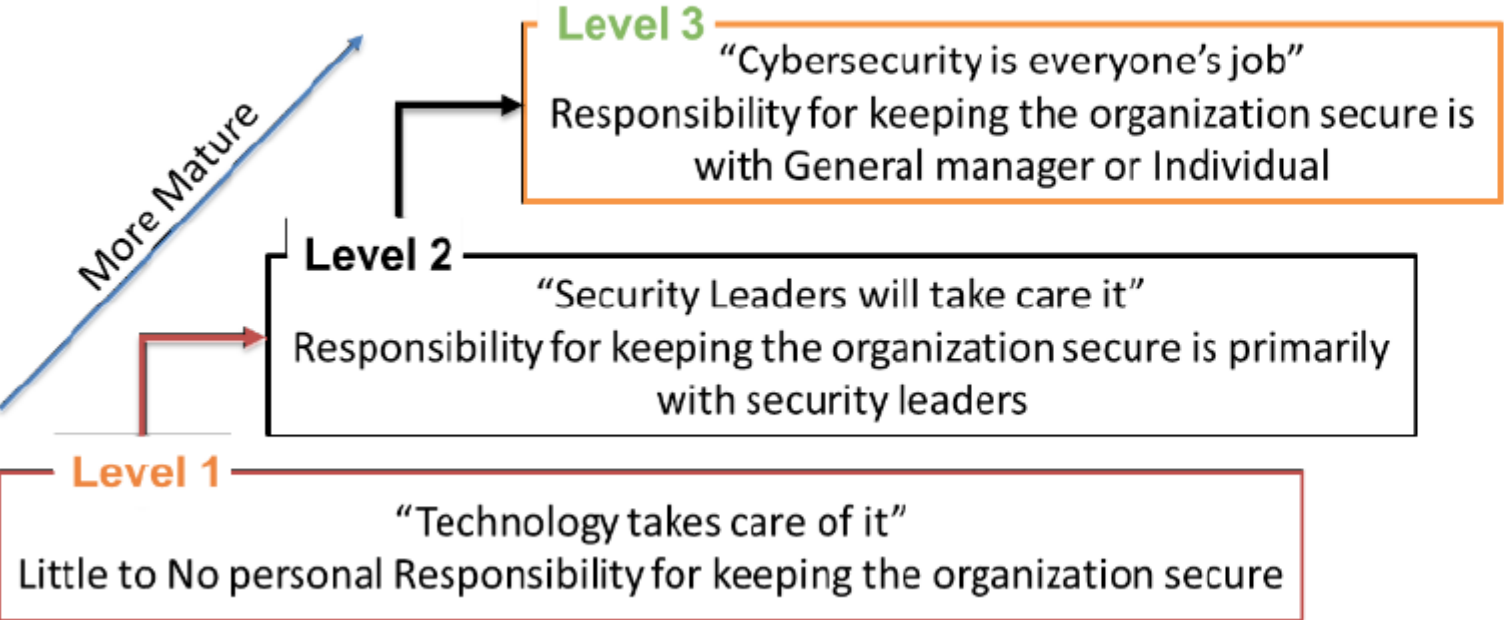
# Organizational Cyber Culture Model (MIT SLOAN)

Figure iii.1: Survey Results (ALL) Heat Map



# MIT Sloan Survey Result

Figure iv.1: Cybersecurity Culture Level based on Responsibility Perception



# Penutup

- Manusia merupakan titik terlemah dalam Keamanan Siber
- Serangan siber terjadi setiap saat dan makin meningkat
- Diperlukan kesadaran **bersama** atas RESIKO serangan siber
- Umumnya tingkat kesadaran keamanan siber masih rendah
- Perlu dikembangkan budaya keamanan siber dilingkungan ASN

**TERIMA KASIH**

# Sumber sumber

- <https://news.detik.com/berita/d-5030865/viral-dugaan-13-juta-data-bocor-ini-tanggapan-kemendikbud>
- <https://www.cnnindonesia.com/teknologi/20200521223601-185-505726/23-juta-data-kpu-diduga-bocor-dijual-di-forum-hacker>
- <https://tekno.tempo.co/read/1501923/kronologi-kebocoran-data-pengguna-aplikasi-e hac-hingga-akhirnya-dinonaktifkan/full&view=ok>
- <https://tekno.kompas.com/read/2021/06/11/13040057/kasus-kebocoran-data-279-juta-wni-bpjs-kesehatan-akan-digugat-lewat-ptun?page=all>
- <https://www.liputan6.com/tekno/read/4449390/lebih-dari-125-ribu-data-mahasiswa-undip-bocor>
- <https://tekno.kompas.com/read/2021/04/04/09330067/data-533-juta-pengguna-facebook-bocor-termasuk-indonesia?page=all>
- <https://www.infosecurity-magazine.com/news/mustang-panda-compromises/>
- <https://nasional.kompas.com/read/2021/09/14/10535821/bin-bantah-servernya-diretas-hacker-china?page=all>
- <https://nasional.kompas.com/read/2021/09/14/10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber>