ITU FINANCIAL INCLUSION AND DIGITAL FINANCIAL SERVICES SECURITY LAB

Asia-Pacific Regional Development Forum

13-15 September 2023, Bangkok, Thailand

Passwordless Blockchain Secure Authentication Secure, Fast and Convenient

Thaib Mustafa, Director & CEO, FNS (M) Sdn Bhd
and
Nurzulaikha Zulkifli, Senior Systems Engineer
FNS (M) Sdn Bhd

Presentation Agenda

01 Introduction – FNS Value Company Limited

02 Security, Trust & Resiliency - The Era of Disruption

03 Passwordless Authentication - Are we ready?

04 Blockchain Secure Authentication – Secure, Fast & Convenient

05 BSA Sandbox – Explore the Future of Web 3.0

01

Introduction

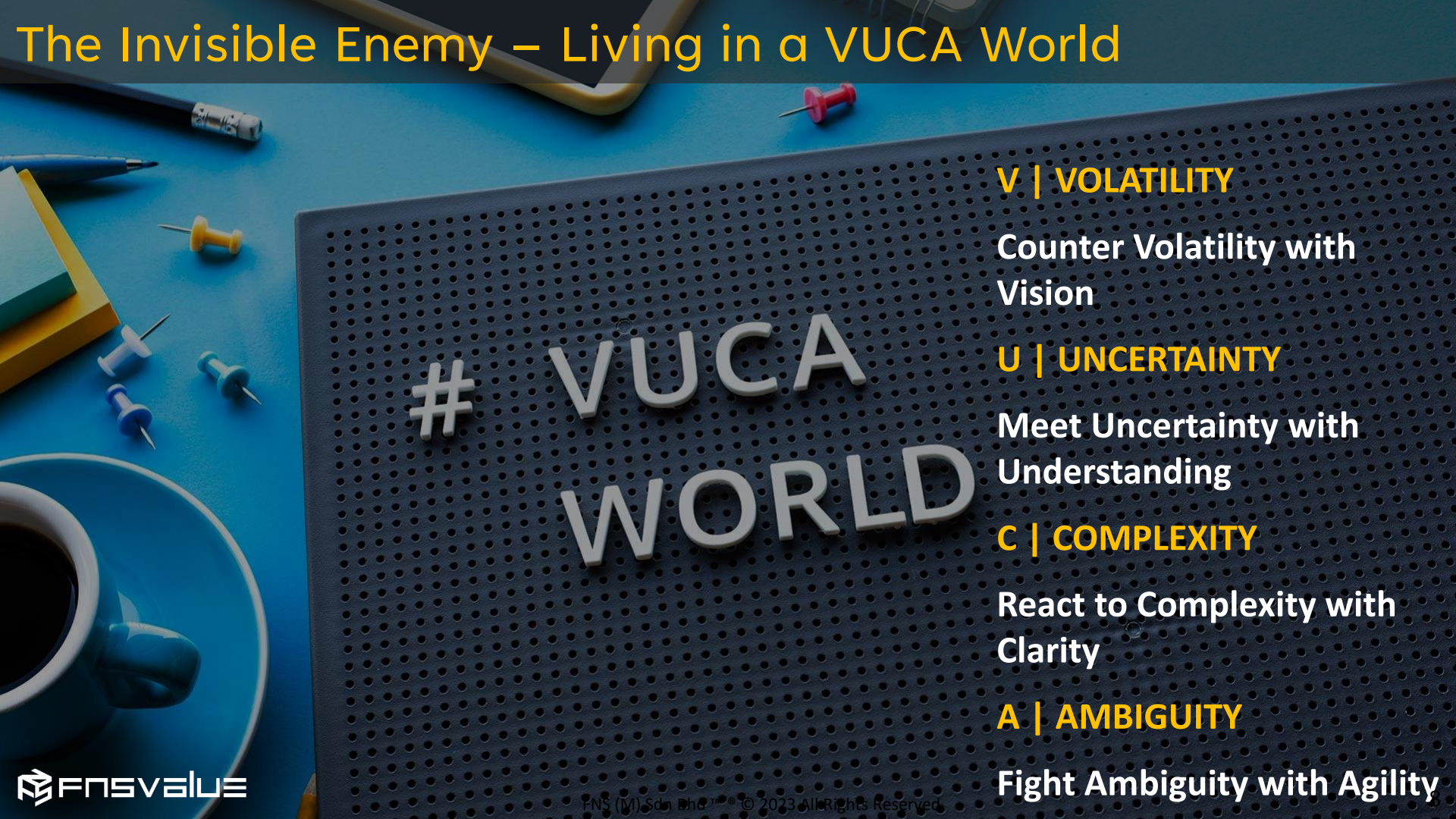
FNS Value Company Limited

About us

- FNS VALUE Company Limited (FNSV), Republic of Korea is the principal of Passwordless Blockchain Secure Authentication or BSA solution with a vision of securing digital services access based on Distributed Ledger Technology (DLT) blockchain based One Time Security Key (OTSK) for a secure, fast and convenient access to web and mobile applications.
- FNS (M) Sdn Bhd (FNSM) is a wholly owned subsidiary of FNSV, based in Kuala Lumpur, Malaysia to serve the regional market as the BSA Center of Excellence.
- BSA has emerged as the forefront leader in passwordless authentication and a trailblazer in blockchain based access security. With extensive deployments of more than 2 million users, BSA safeguards organizations across public and private sectors including Critical and Network Information Infrastructure (CNII) with cross vertical use cases from digital financial services to academia, ensuring user and consumer privacy protection, securing digital access while maintaining fast and convenient user interface and experience (UI/UX).

Security, Trust & Resiliency
The Era of Disruption
02

The Invisible Enemy – Living in a VUCA World



V | VOLATILITY

Counter Volatility with Vision

U | UNCERTAINTY

Meet Uncertainty with Understanding

C | COMPLEXITY

React to Complexity with Clarity

A | AMBIGUITY

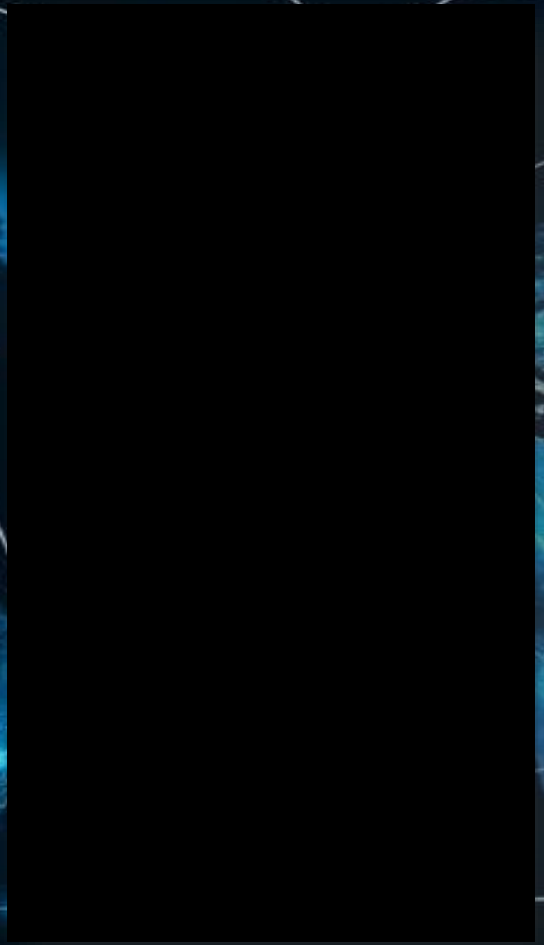
Fight Ambiguity with Agility

Are we secure enough?

- We heard about it
- Well informed
- We were advised
- We talked about it
- And we understood

The Question is on Cyber Resiliency:
How fast can you identify, **protect**, detect, respond and recover from cyber attack? – NIST CSF1.0

Let’s catch a short video ::



Cyber attacks is the New Normal

FNSVALUE

A Quick Statistics & Incidents
Source: ITU Pacific CyberDrill

Global CNII Cyber Attacks

2009 - 2020

2009
Ministry of Defence
- Conficker

2010
Nuclear facility
- Stuxnet malware

2012
Oil refineries
- Flame Malware

Gas facility
- Shamoon virus

Oil refinery
- Shamoon virus

2014
Steel mill ICS
- Spearphishing email

2015
Power grid
- Spearphishing + BlackEnergy 3 Malware

2016
Power grid
- GreyEnergy

Power grid
- Industroyer

Water company
- PLCs were compromised by hackers

2017
Car manufacturer
- WannaCry Ransomware

Metro & airport
- NotPetya + BadRabbit

Shipping Company
- WannaCry Ransomware

Oil company
- WannaCry Ransomware

Pharmaceutical company
- WannaCry Ransomware

2018
Oil service company
- Shamoon virus

2019
Power grid
- Hacked the power grid

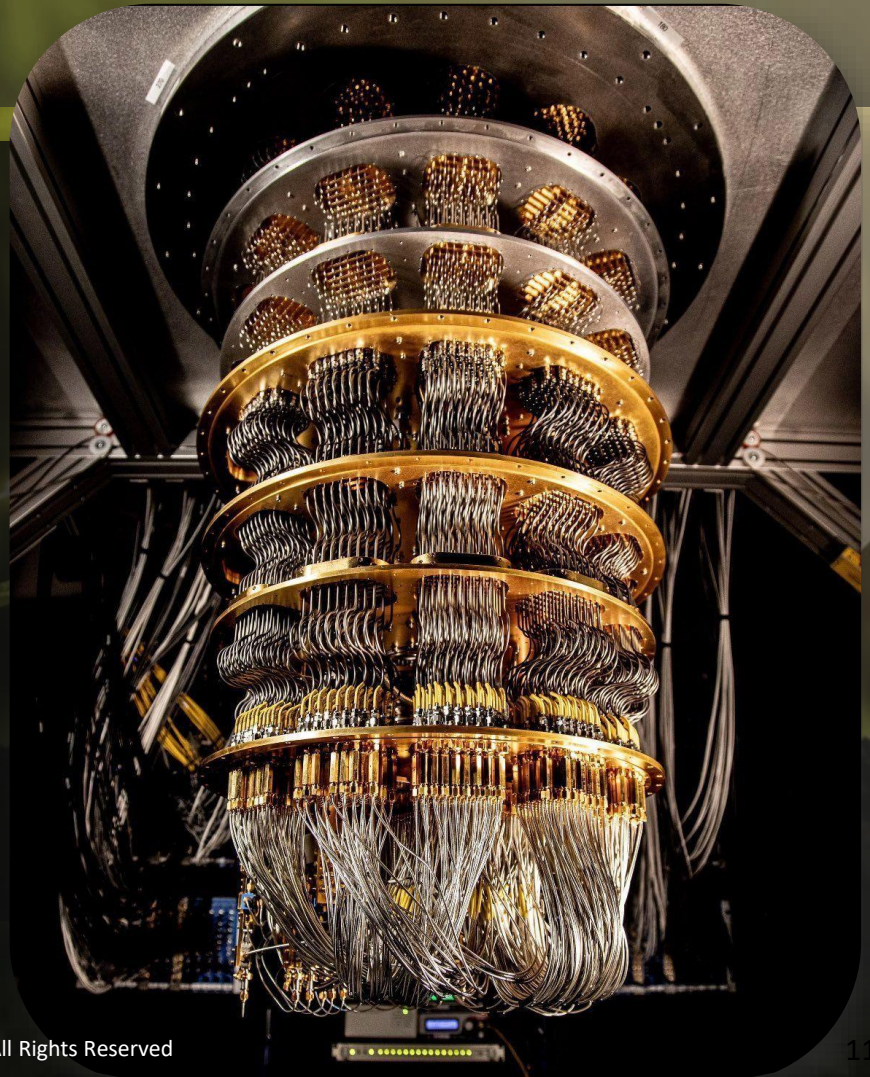
Commercial vessels
- Malware attacks using phishing to steal info on vessels and voyage

2020
Water system
- Hacked the water pump stations

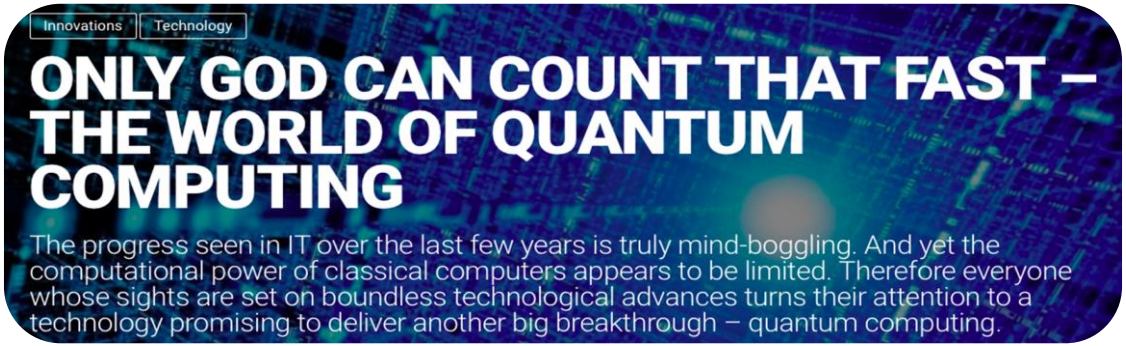
Internet service provider
- Ransomware attack by REvil ransomware gang

Quantum Computing

- Google New Quantum Computer. 47 years faster than #1 supercomputer today.
- Ability to perform in 200 seconds calculation that the world's fastest supercomputer that will takes 10,000 years to complete.
- Huge potential of quantum computing in solving complex problems much faster than classical computers.
- Google is currently using it to solve optimization problems and finding the best outcome given a set of data.



"About 25% of bitcoins and 65% of ether coins could be vulnerable to a quantum attack, putting more than USD40 billion of value at risk." - WEF



"Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built." – ETSI

"The precise threat timeline you should focus on depends on your risk tolerance. For very critical systems and assets, the likelihood of quantum attacks in five years is becoming material and for most critical systems and assets I believe the 10-year likelihood needs to be addressed assertively." - Michele Mosca, University of Waterloo, Canada

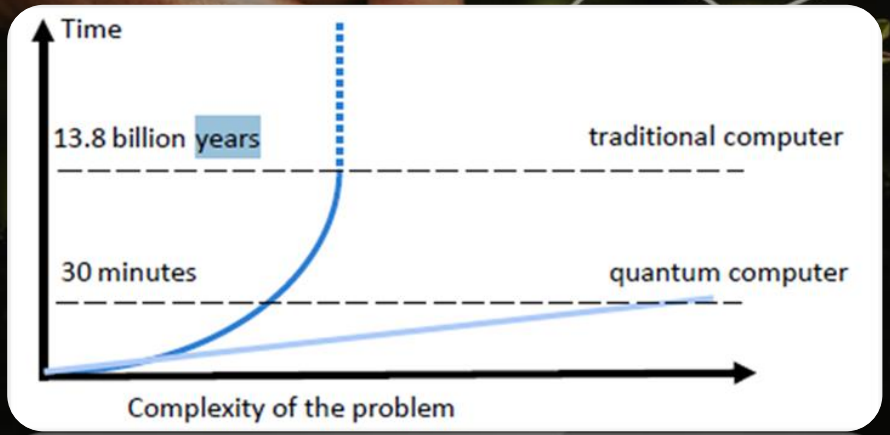
Protecting our private communication isn't just about keeping our banking information safe. It's preserving our right to share information, learn about the world around us, and make informed decisions for the benefit of society.

Quantum Computing | Evolution

Quantum mechanics, beginning of 20th century explains foundational concepts of how basic matter exists, changes and interacts over time.

1st quantum revolution - quantum properties were used to manufacture superior devices (lasers, transistors, etc.). 2nd quantum revolution refers to storage and processing of information in quantum devices.

Emerging quantum technology have the capacity to drive high-impact use cases and advanced applications such as **quantum computing, quantum sensing and quantum communications.**



- October 2019, **Google in partnership with NASA** demonstrated ability to compute a problem that can only be solved by quantum computer in seconds. A milestone known as **Quantum Supremacy**.
- August 2020, **IBM reached a new quantum computing milestone**, hitting its highest Quantum Volume and plan to release cryptanalytically-relevant **quantum computers in 2023-2025**.
- **China is particularly active in quantum technologies** having the leading number of patents registered; reflecting the fact that **Quantum Technology is the new battle among world superpowers.**
- May 2022, **NSA Director, "cryptanalytically-relevant quantum computer could jeopardize civilian and military communications** as well as undermined supervisory and control systems (SCADA) for critical infrastructure. The number one defense against this quantum computing threat is to implement **quantum-resistant cryptography**…"

Quantum Computing | Impact on Critical and Network Information Infrastructure (CNII)

Sector at risks with traditional (i.e. non-quantum) cyberattacks

Telecoms (4G and 5G)

- **Global value of the market currently at risk: $2.71 trillion[3].**
- Cyberattacks on telecoms are popular because their databases carry detailed information on millions of customers.
- A successful data breach could yield contact details, social security numbers, and credit card information – a goldmine for dark actors.

Electronic payments

- **Global value of the market currently at risk: $70 billion[4]**
- Cyberattacks can happen at any level of the payment processing industry and can have far-reaching implications.
- As more consumers embrace new methods of payment, questions over cybersecurity have become even more critical for businesses

E-commerce

- **Global value of the market currently at risk: $11 trillion[6]**
- Since e-commerce companies store customers' personal information in their systems, they are particularly vulnerable to cyberattacks.
- Bank account and credit card information, mailing addresses and passwords are all used by cybercriminals for identity theft and fraud

Financial Services

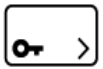
- **Global value of the market currently at risk: $22 trillion[7].**
- Financial services companies are a prime target for cyberattacks as they have a huge stores of highly sensitive, personally identifiable data that can be leveraged and monetized by cybercriminals.

E-Govt

- **Global value of the market currently at risk: $57 billion[5]**
- These attacks are perpetrated to compromise Government networks, steal financial & intellectual property, and put critical infrastructure at risk – i.e.: cyberwarfare.

Aerospace & Defense

- **Global value of the market currently at risk: $700 billion[8]**
- The sector has become the target of particularly sophisticated and ruthless actors in the cyber space – very often state-sponsored.



Insurance

- **Global value of the market currently at risk: $5.05 trillion[9]**
- These are natural target for cyberattacks because they possess substantial amounts of confidential policyholder data.
- Lloyd's Insurance has recently slashes coverage for state-sponsored attacks - reflecting the impact of ransomware attacks on the industry

Note: 1 Allianz Global Corporate & Specialty, 2 Blackfog, 3, 4, 5 Globe news wire as of 2021, 6 Grand view research as of 2021, 7 -Business wire: Global financial services outlook as of 2021, 8 -PWC IndustryReport as of 2021, 9 –Statisticaas of 2021

The Power of AI | Bots are better than humans at cracking ‘Are you a robot? Captcha tests study finds

- Bots are now outperforming humans in Captcha tests, a security measure designed to differentiate between human users and automated bots.
- Advanced machine learning models have achieved an accuracy of 90%, surpassing the average human accuracy of 87%.

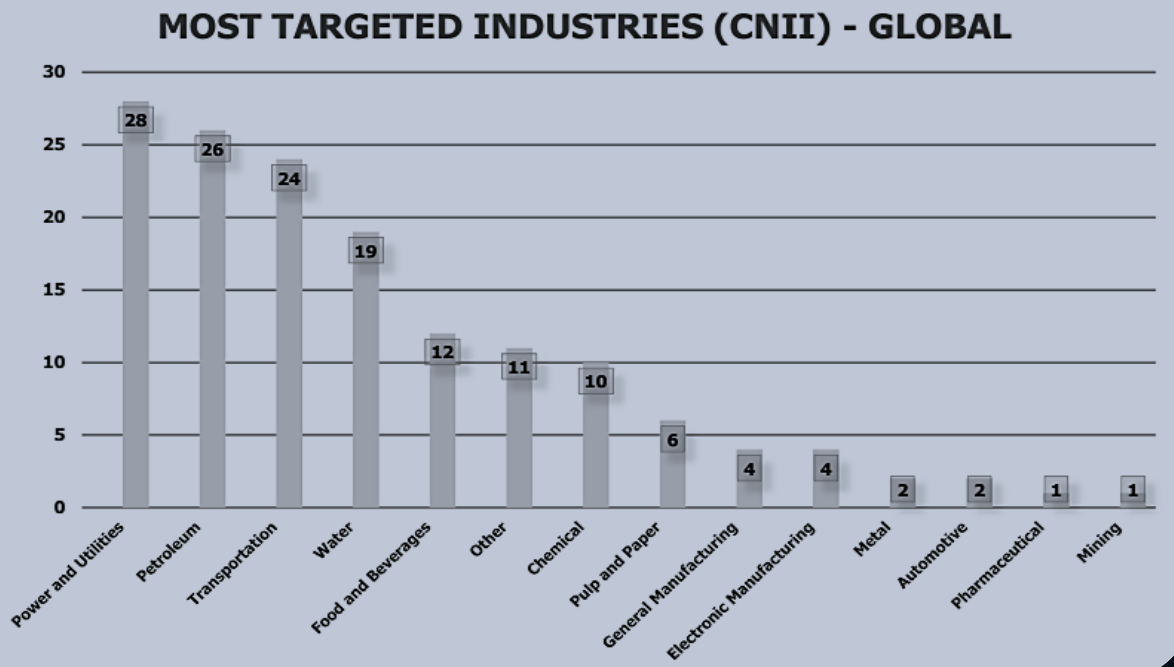
Global Security Landscape

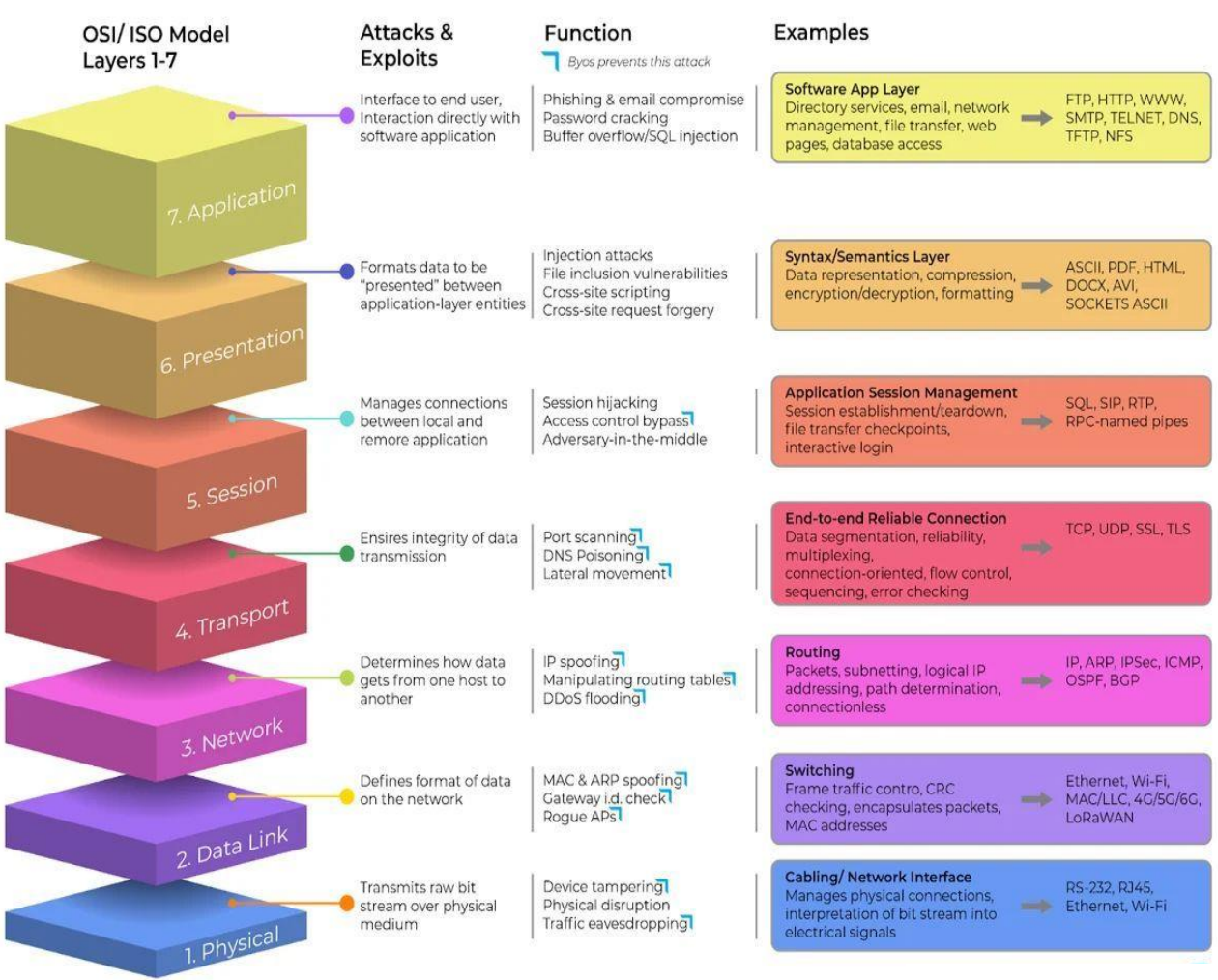
A Quick Statistics & Incidences
Source: ITU Pacific CyberDrill

THREATS AND ATTACKS

Most Targeted Industries

Global Statistics





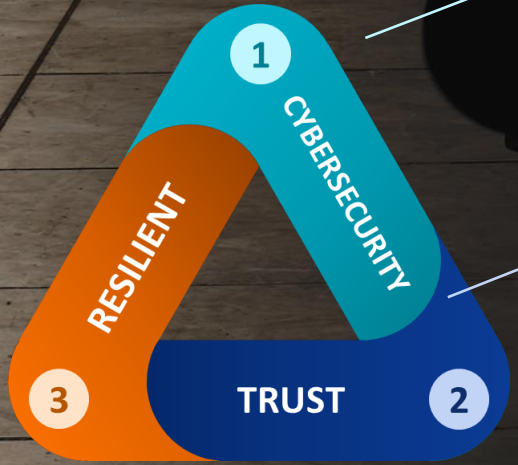
Attack surface on OSI/ISO 7 Layers

Cyber Resilience for a Brave New World?

- **What?** Cyber resilience is the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems - National Institute of Standards and Technology (NIST).
- **Purpose** of cyber resiliency is to ensure that business processes can continue to function smoothly in a contested cyber environment.
- **The whole process** - Cyber resilience is a key part of culture, processes, and decision-making to be ever ready for managing the risks of compromise, reputational damage, and financial damage.
- **Continuity** - Organisation to proactively address future potential business continuity challenges, including natural disasters, economic crises, cyber security incidents, and other unforeseen events and enable effective response and recovery mechanisms are ready for near-instant activation.
- **Contingency** - Organisation to ensure contingency capabilities are available to recover from threats that could impact the distribution of human, technical, third-party and data resources, with critical impact to the business and its services.
- **Planning** - Cyber resilience planning is especially important in all convergence technology (IT, OT, NT, IoT, etc.) environments, where hardware and software interact with the physical world and support public services. These systems need to be resilient to cyber security failures and failures of other types as well.
- **Initiatives** - Embarking on new resilience initiatives may seem daunting, but a series of resources can assist. Examples include the World Economic Forum's Cyber Resilience Index, NIST's 800-160v2, MITRE's Cyber Resilience Engineering Framework, and Cyber Talk's operational resilience recommendations
- **Prevention** - As organizations look to prevent a growing number of complex and evolving cyber security threats, operational resilience is becoming a top priority for leaders.
- **Non-Exception** - An organization's level of operational resilience is contingent upon the organization's ability to adapt to, respond and recover from disruptive events — from cyberattacks to natural disasters to other incidents — without compromising essential operations.

Security, Trust and Resiliency

Critical for Business Sustainability



1

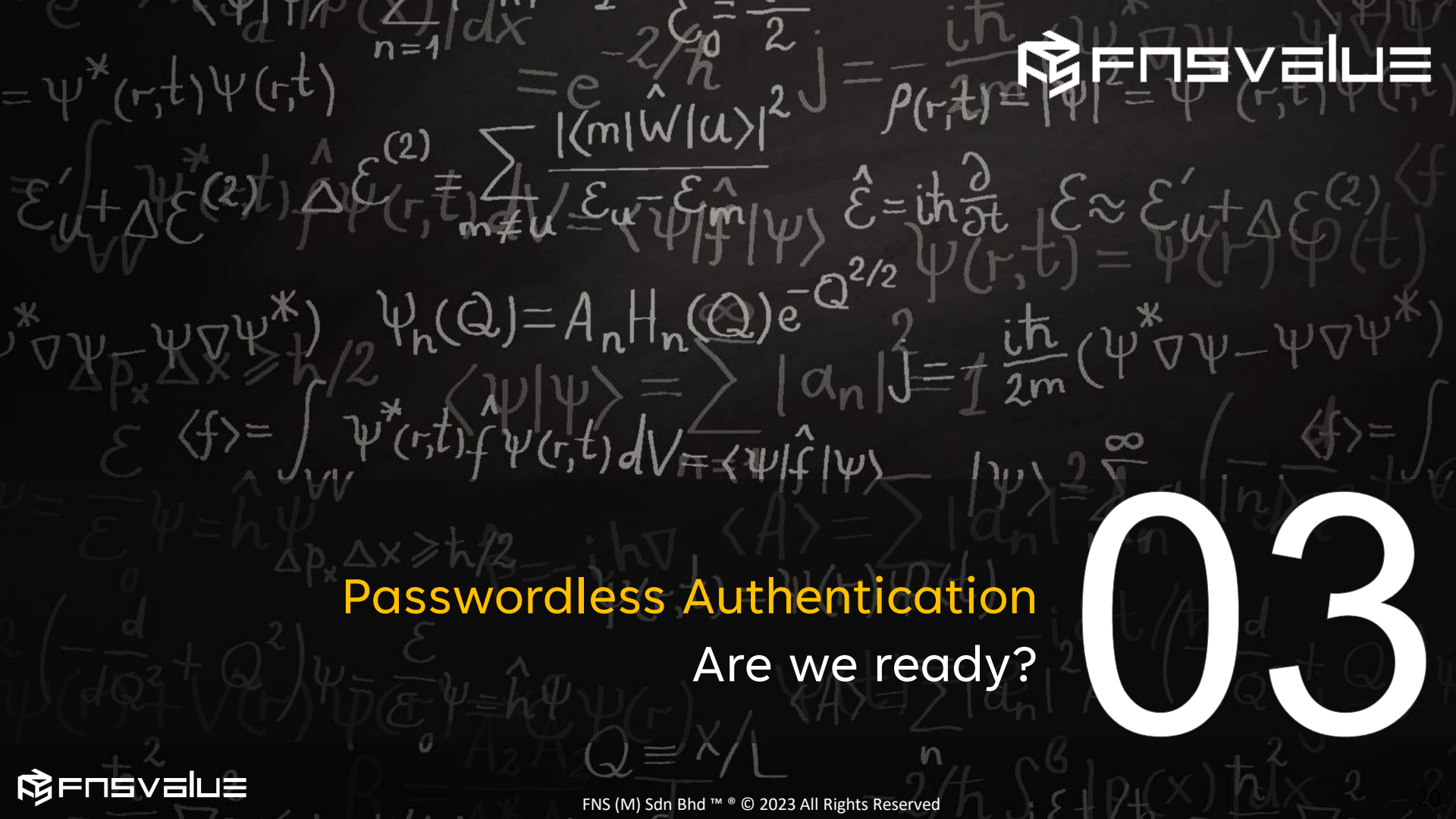
- Process, Technology & People
- Good and Best Practices
- Physical & Virtual Environments
- Governance, Risks & Compliance

2

- Trust is an Assurance
- Trust as a measure of Trustworthiness
- A Trusted Systems, Process & People
- A Trusted Brand & Organisation

3

- Ability to anticipate, withstand & recover from adverse conditions
- Ability to prepare for, respond to & recover from worst case scenario
- Business Continuity & Sustainability



Passwordless Authentication

Are we ready?

03

Global Cybersecurity Outlook 2023

World Economic Forum (WEF) in collaboration with Accenture surveyed **117 cyber leaders** in **32 Countries** over **22 Industries** and examined cybersecurity trends that will impact economies and societies in the future. Report findings are as follows:

Source: World Economic Forum

93%

cybersecurity leaders and 86% of business leaders believe a cyber catastrophe is likely in 2 years

74%

cyber and business leaders surveyed said that they expect to face more cyberattacks in 2023 than in 2022.

USD4.24M

Average cost of authentication-related cyber breaches

26%

of cyber threats come from access security vulnerabilities

Cybersecurity threats are inevitable

The current state of cybersecurity in 2023

USD8 Trillion

Cost of cybercrime predicted in 2023

Source: Cybersecurity Ventures

4,741

Cases of cyber threats in Malaysia, 2022

Source: Cybersecurity Malaysia

USD6 Million

Malaysia's total loss as of February 2023

Source: Cybersecurity Malaysia

8th/165

Malaysia's ranking in terms of cyberattack vulnerability

Source: NordVPN

2023 Ransomware Trends Report

An independent research firm surveyed **14 Countries** and **1,200 unbiased IT leaders** about the impact that ransomware had on their environments, as well as what their IT strategies and data protection initiatives are moving forward.

Source: Cybersecurity Ventures

74%

Organizations had authentication-related breaches in the last 12 months

32%

IT helpdesk cost related to password issues - on average of USD375/employee

USD2.95M

Average cost of authentication-related cyber breaches in the last 12 months

28%

Organizations were hit by push notification attacks (MFA bombing), more than double vs. reported last year

Why target cloud environments?

Multi-cloud environments are complex and therefore
more difficult to protect

Rapid software delivery processes make cloud-native apps
susceptible to vulnerabilities and misconfigurations

Rogue and shadow cloud environments
lack security controls and oversight

Siloed security point products leave blind spots
adversaries can slip through unnoticed

Threat actors are cloud-savvy and refine their tactics to abuse cloud services and exploit cloud vulnerabilities. Here are the top three cloud attack techniques observed by the CrowdStrike Threat Intelligence team over the past year while tracking 200+ threat actors.

Identity Is a Key Cloud Access Point

Threat actors are seeking new ways to leverage identities in the cloud

43%

Adversaries are becoming more reliant on valid accounts, which were used to gain initial access in **43%** of cloud intrusions observed.*

67%

In **67%** of cloud security incidents, CrowdStrike found identity and access management roles with elevated privileges beyond what was required — indicating an adversary may have subverted the role to compromise the environment and move laterally.*

47%

Nearly half (47%) of critical misconfigurations in the cloud were related to poor identity and entitlement hygiene.*

Source: Crowdstrike

2023 Ransomware Trends Report

There are **4 critical areas on access security** that impact directly on organizations **State of Access Security**:

Source: Cybersecurity Ventures

1

Weak Authentication Methods

Out of 74% of breaches, 82% are strongly related to **credential misuse** or authentication weakness.

Famous tactics: MFA Bombings

2

Traditional Authentication Methods

57% of workforces are still on 1st Generation – User ID and Passwords.

Famous tactics: Social Engineering

3

Perception and Beliefs

35% - Completely secure

53% - Mostly secure

12% - Somewhat secure

Majority of IT and security leaders believes their organization to be completely or mostly secured.

4

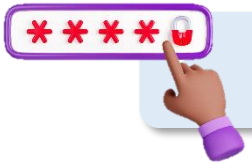
True Passwordless Authentication

97% of 'passwordless' solutions deployed are susceptible to **phishing** and **push attacks.**

A True Passwordless Authentication enhances security layers without requiring a centralized based primary security key or a 'Master' key.

How effective are the current access security measures?

The challenges and limitations of the existing access security controls:



Passwords are easy to forget, steal, or hack.

Multi-factor authentication (MFA) adds complexity and inconvenience for users. Devices can be stolen.

Biometrics can be spoofed or compromised. Deep Fake.

Centralized databases are vulnerable to breaches or attacks. Insider Threats.

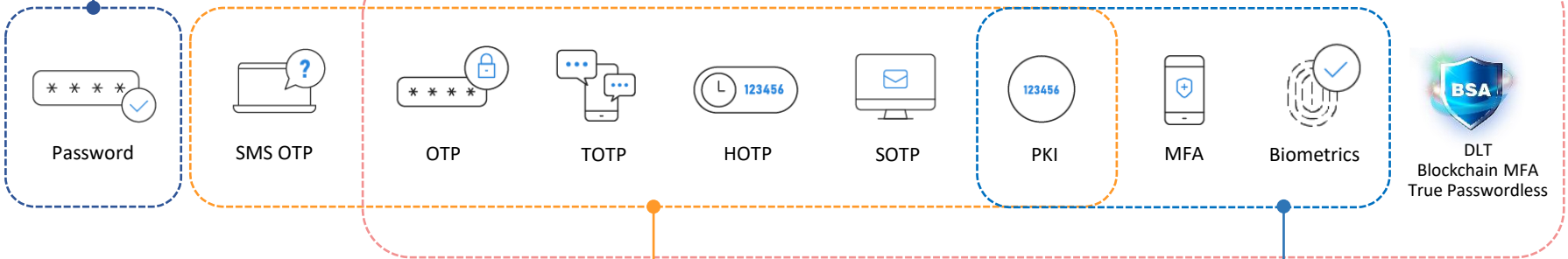
Authentication Security Evolution

1st Generation

Password-based Authentication
- 1FA (User ID & Password)

4th Generation

Passwordless Blockchain MFA (OTP ~ Biometric)
True-Passwordless (Non-PKI-Based, No Master Key)
True Frictionless (Fast and Convenient)
One-Time Security Key (Decentralized Depository)
Distributed Ledger Technology (DLT) Authentication



2nd Generation

One-Time Password/Token Based Authentication
2FA (SMS, OTP, TOTP, HOTP, SOTP)
Certificate Based Authentication - 2FA (PKI)

3rd Generation

Biometric Authentication - 2FA (Face, Fingerprint)
Multi-Factor Authentication - MFA (PKI, Biometric, Token)
Centralized Depository – Master Key, Password or Passwordless

Challenges and Issues on Authentication Security

1FA: User ID and Password

Issues: Human Error, Too many passwords
Known Attacks:
Keylogger attacks, phishing attacks, and Man-In-The-Middle attacks (MITM)

1FA: User ID and Password
2FA: Certificate or Token-Based

Issues: Managing and Tracking PKI, Costs of operating (SMS, etc.)
Known Attacks:
Malware disguised as software update, Spyware for SMS Divert and MITM

1FA: User ID + Device + Password / User ID + Device + OTP Codes
2FA: Biometrics

Issues: Centralised user data & information, Credentials & Master Key/Password
Known Attacks:
Compromised assets and devices

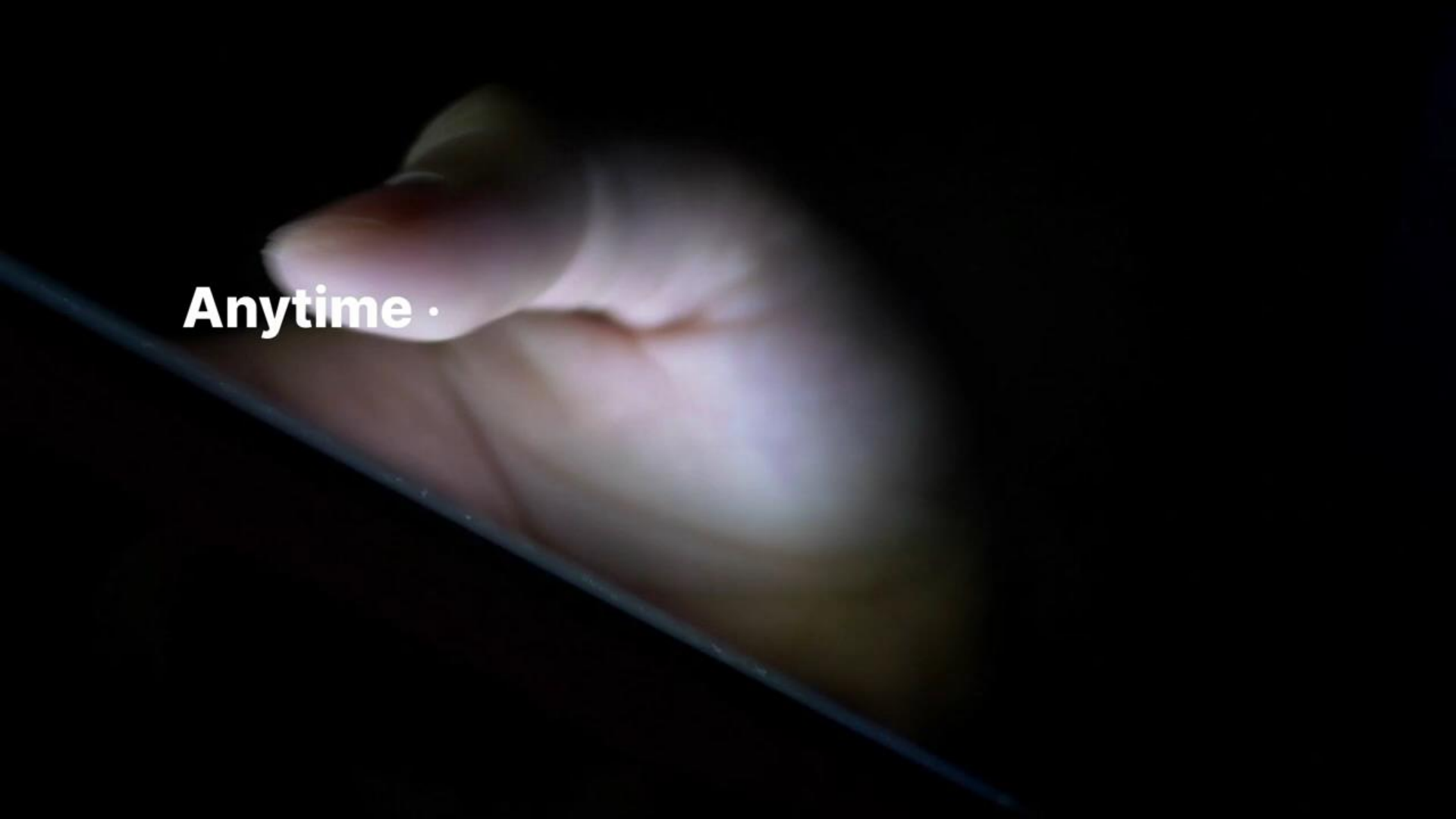
1FA: User ID + Device (via Blockchain Nodes, Biometrics)
2FA: MDV and DLT OTSK
3FA: Biometrics

Issues: Emerging Technology
Known Attacks: None
Advantages: No Passwords Required, Decentralised Random Credentials, Virtual OTSK, Distributed Random Verification, Hybrid Blockchain Network.

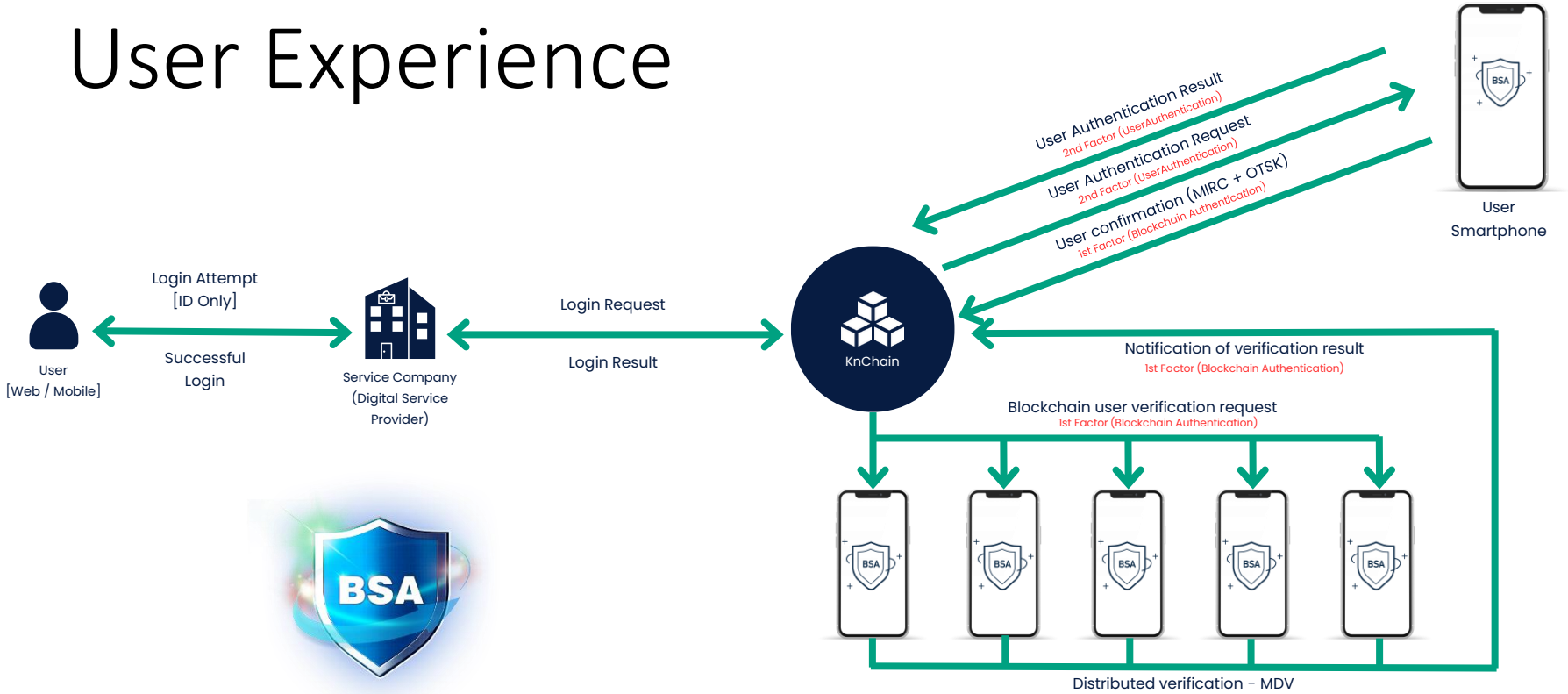
Blockchain Secure Authentication

Secure, Fast & Convenient

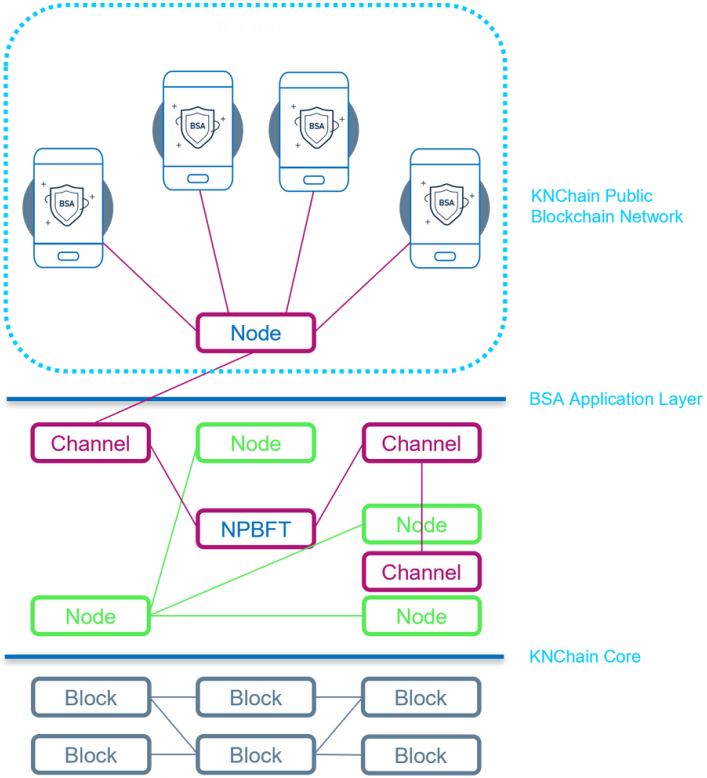
04


Anytime ·

BSA Passwordless User Experience



BSA Technologies



Multiple Random Identifier Random Combination (MIRC)

Passwordless BSA server extracts unique identifier from user device and combine multiple identifiers data sources to generate One Time Security Key (OTSK).

One Time Security Key (OTSK)

OTSK is a volatile runtime key that is generated in MIRC and encrypted with 3 layers of encryption.

Multilateral Distributed Verification (MDV)

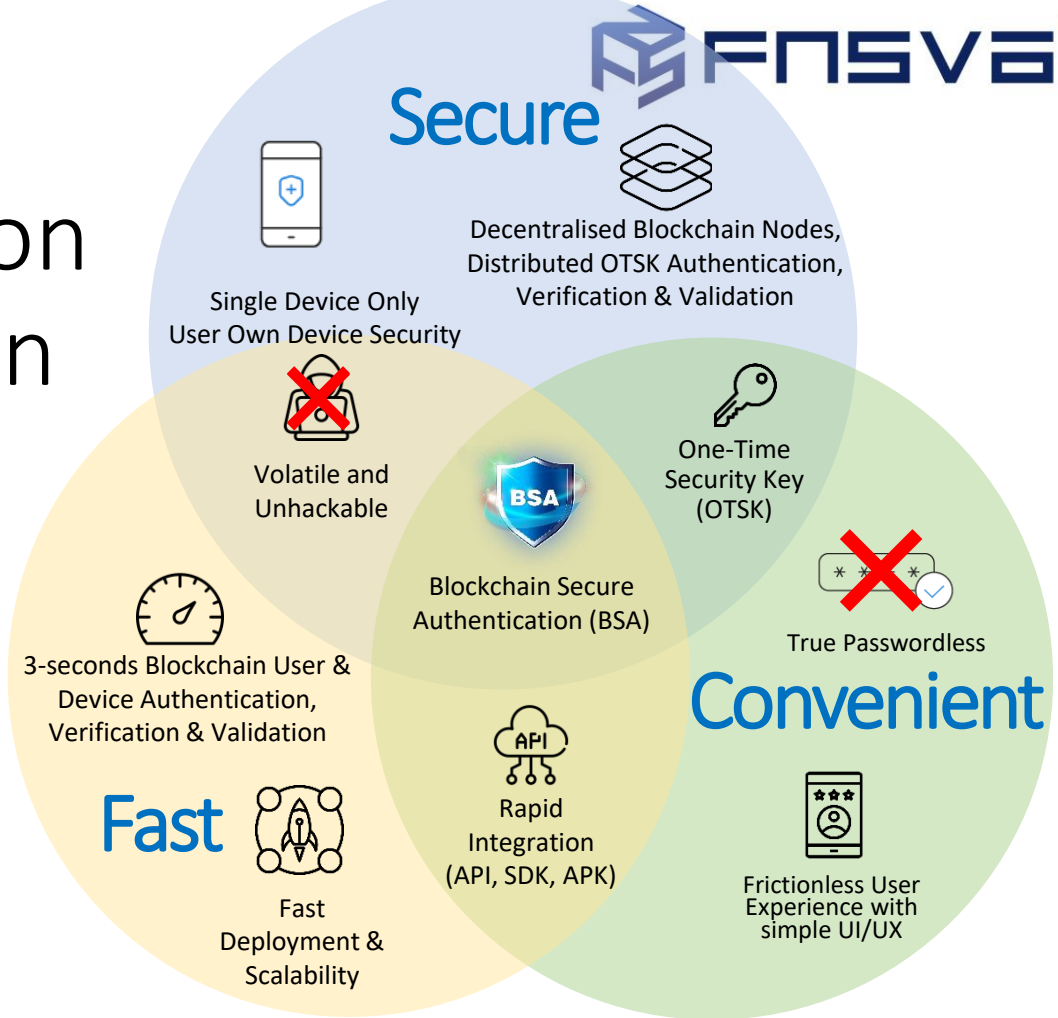
Passwordless BSA OTSK is verified with a randomly distributed verification process of registered mobile devices to verify user access.

Kernel Chain (KNChain)

Passwordless BSA used a hybrid blockchain network with 3 major authentication requirements: Trust, Performance, Security.

Blockchain Authentication is the solution

- Revolutionizes access security in the digital landscape.
- Ensures maximum security, faster deployment, scalable and convenient UI/UX.
- Provide an effective and efficient solution for safeguarding the crown jewels of organization's data with security, trust, resiliency.



BSA for Web 3.0
Digital Access Security

DLT with blockchain passwordless based authentication will revolutionize access security in the digital world:

Financial Institutions

Protect from unauthorized access or tampering – Bank Negara revised RMiT, regulated to comply with highest level of authentication technology & process possible.

Government

Protect government data from unauthorized access and tampering – many government assets and data is sold to dark web due to weak authentication

Sources: Forbes, World Economic Forum, Harvard Business Review

Information & Communications

Protect privacy of data through decentralization to secure from unauthorized access – comply to Privacy Regulations, GDPR, PDPA, etc.

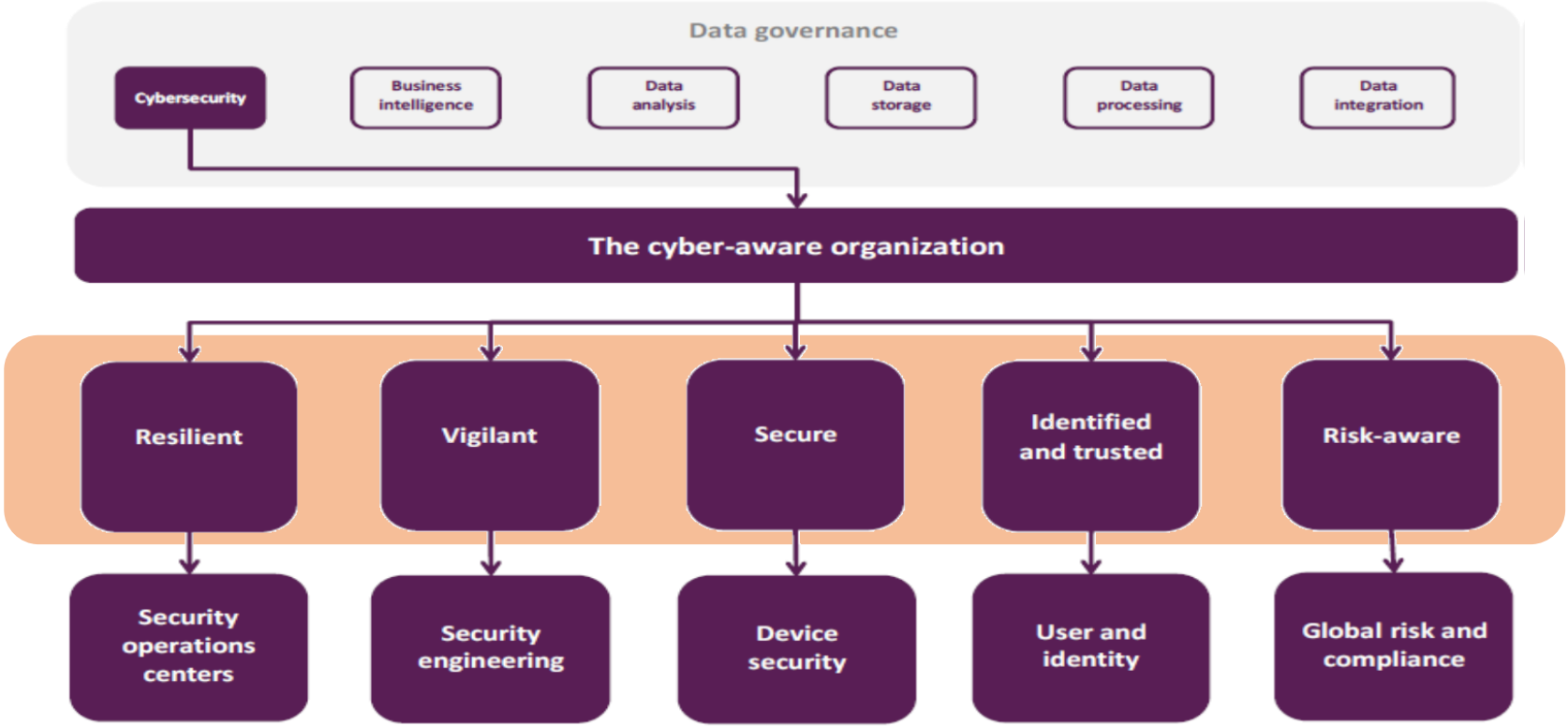
Healthcare

Protect access to critical data – cannot be protected with current centralized way of authentication

Cyber Resilience & Zero Trust | Key Operational Strategies

1. Proactive risk management.
2. Strong identity and access management.
3. Threat intelligence and information sharing.
4. Incident response and business continuity planning.
5. Cloud security and migration strategies.
6. Continuous monitoring and evolution.

Web 3.0 Requirements: Security, Trust & Resiliency by Design



05

BSA Sandbox

Explore the Future of Web 3.0


FNSvalue
www.fnsbsa.com
THANK YOU
“Let’s go passwordless”
Blockchain Secure Authentication (BSA)
Secure, Fast and Convenient