

SEMINAR

VIETNAM'S PDPD

NAVIGATING THE IMPACT OF VIETNAM'S PDPD ON CUSTOMER DATA MANAGEMENT



Mr. ANDREW QUACH
Director of Consulting
AHT Tech Joint Stock
Company



Mr. EDDY BELLAVOINE
Chief Commercial Officer
SafeComs Network Security
Consulting Co., Ltd



Ms. THACH TRAN
Senior Manager
EY Law Vietnam
Limited Liability Company



Co-organizers



Speakers



Venue Sponsor



Decree 13: Key considerations for domestics and foreign businesses in Vietnam

Ho Chi Minh City

Wednesday, 28 February 2024

Speaker



Thach Thi Cam Tran

Senior Manager

EY Law Vietnam Limited Liability Company



Building a better
working world

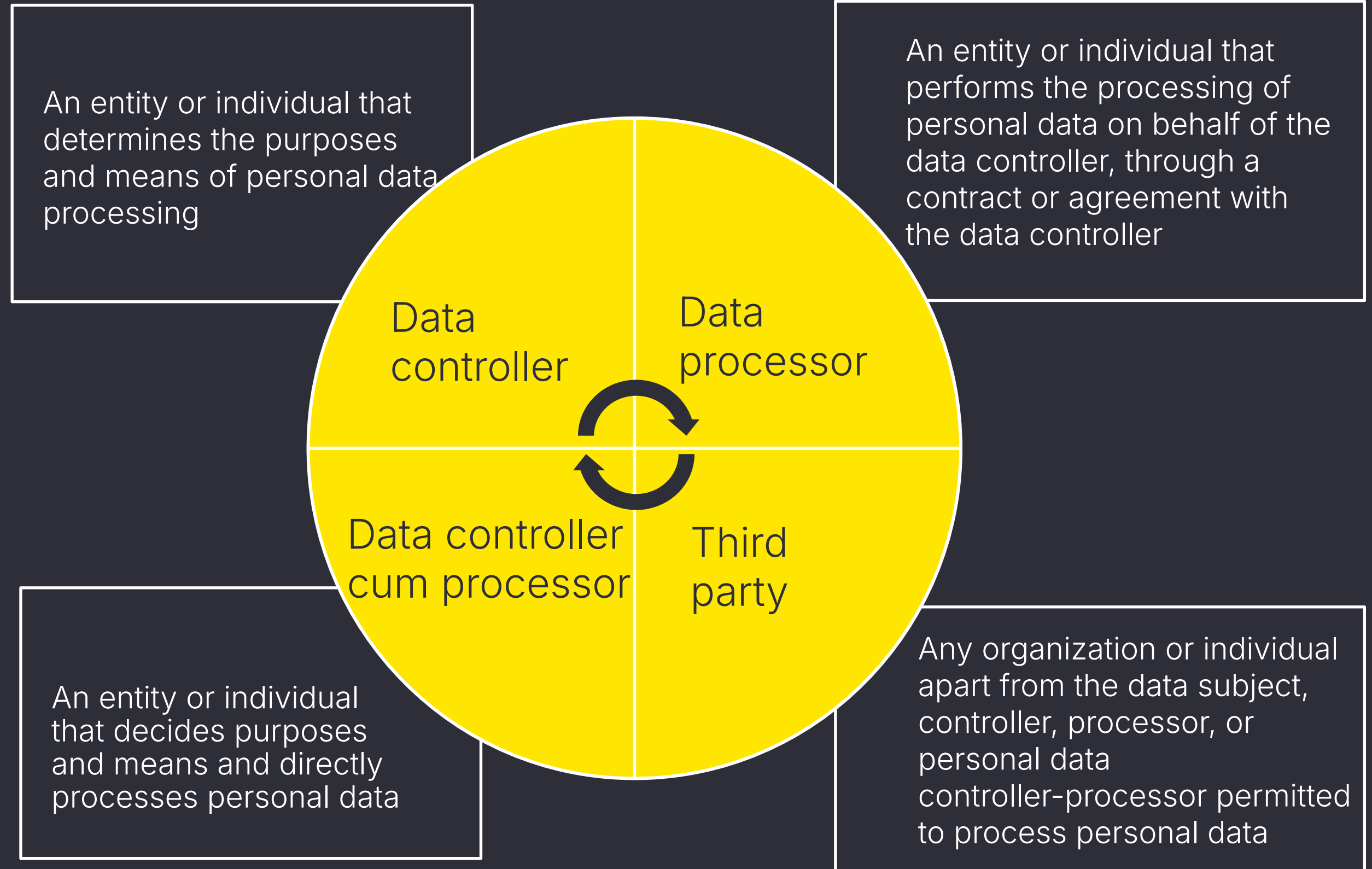
Disclaimer

- ▶ This material has been prepared for general informational and educational purposes only and is not intended, and should not be relied upon, as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.
- ▶ Neither the EY organization nor any of its member firm thereof shall bear any responsibility whatsoever for the content, accuracy, or security of any third-party websites that are either linked (by way of hyperlink or otherwise) or referred to in this presentation.
- ▶ The views of third parties set out in this webcast are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

Key considerations (1/4)

Definition of personal data

Personal data is information in the form of symbols, letters, numbers, images, sounds or similar form on an electronic environment that is associated with a particular individual or helps to identify a particular individual [Article 2.1 Decree 13/2023/ND-CP on personal data protection (Decree 13)]



Key considerations (2/4)

Aspect	Requirement	Action required
<p>Consent requirement</p>	<ul style="list-style-type: none"> Expressed clearly and specifically in writing, by voice, by ticking the consent box, in the syntax of consent by text message, by selecting consent technical settings, or by other actions demonstrating the same Voluntary For single purpose Informed of compulsory contents Affirmative action in a format that could be printed, reproduced in writing, including in electronic form or verifiable format 	<p>To prepare the consent form in line with Decree 13</p>
<p>Personal data processing notification</p>	<ul style="list-style-type: none"> Controller, Controller cum Processor must notify data subject of the processing unless data subject already acknowledged and consented to contents to be notified or the processing by competent authority for their operation in line with laws Notification once prior to the processing with the required contents In a format that can be printed, reproduced in writing, including in electronic form or verifiable format 	<p>To prepare the personal data processing notification with mandatory contents as required by Decree 13</p>

Key considerations (3/4)

Aspect	Requirement
<p>Personal data processing impact assessment</p>	<ul style="list-style-type: none"> Controller, controller cum processor and processor shall submit to a05 personal data processing impact assessment and form 04 within 60 days as of processing date Any changes to the submitted processing impact assessment, controller, controller cum processor and processor shall update A05 respectively <p>Note: Applicable to: (i) controller, controller cum processor (in all cases); (ii) processor (in case of performance of a contract with controller)</p>
<p>Cross-border transfer of personal data</p>	<ul style="list-style-type: none"> The transferors (controller, controller cum processor, processor and third party) shall submit to A05 cross-border transfer impact assessment and Form 05 within 60 days as of processing date Any changes to the submitted cross-border transfer impact assessment, the transferor shall update A05 respectively Upon each successful cross-border transfer, the transferor shall notify A05 information of such transfer and contact details of person in charge <p>Note: Applicable to Vietnamese citizens' personal data only</p> <p>Circumstances: (i) transfer to a location outside of Vietnam, or (ii) using a location outside of Vietnam to process personal data of Vietnamese citizens</p>



Action required
<ul style="list-style-type: none"> To prepare the personal data processing impact assessment with mandatory contents as required by Decree 13 To submit the impact assessment within 60 days as of 1 July 2023 To update the assessment from time to time
<ul style="list-style-type: none"> To prepare the cross-border transfer impact assessment with mandatory contents To submit the impact assessment within 60 days as of 1 July 2023 To notify A05 upon each successful cross-border transfer To update the assessment from time to time



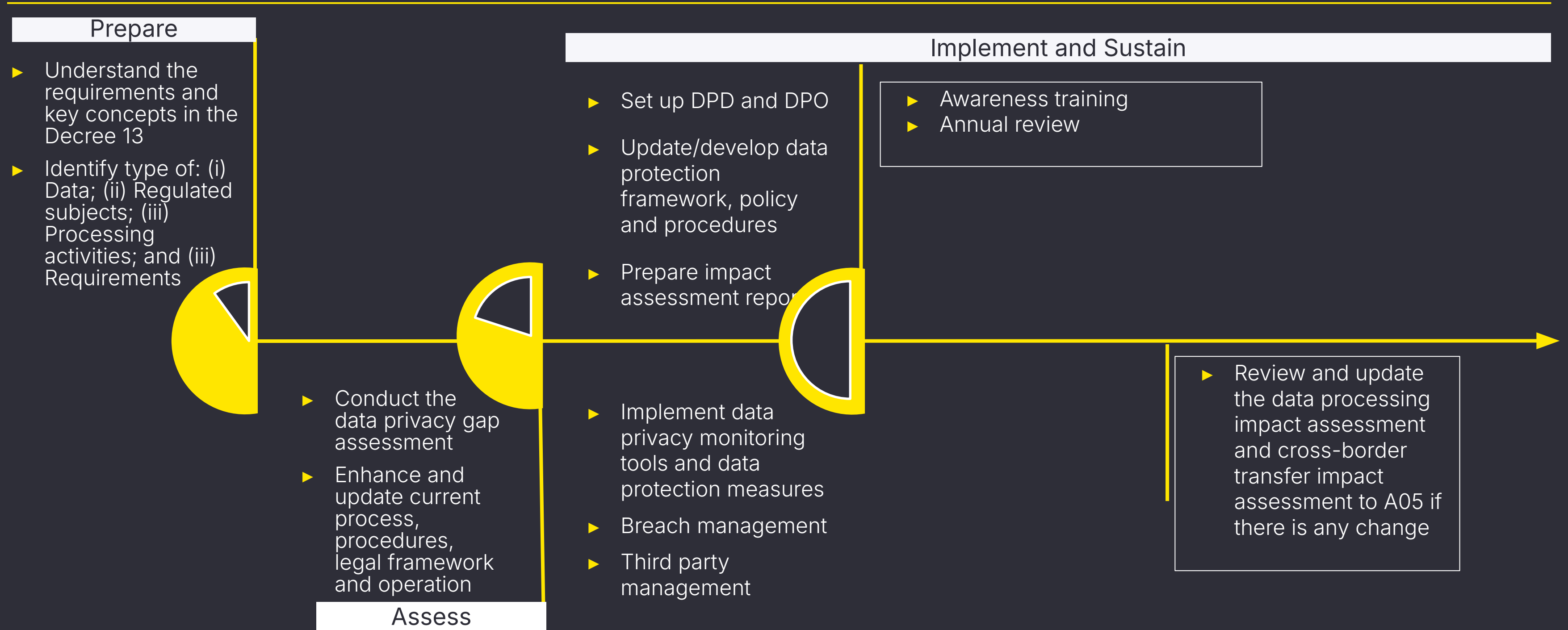
Key considerations (4/4)

Aspect	Requirement
Personal data breach management	<ul style="list-style-type: none"> • The processor shall notify the controller as quickly as possible after detecting the violation • <input type="checkbox"/> The controller or the controller cum processor shall notify the A05 • The controllers, the controller cum processor must make a written confirmation of the occurrence of breach and cooperate with A05 to handle the breach
DPO/DPD appointment	<p>Controller, processor and controlling-processing entity, processor who process sensitive personal data shall appoint a unit specializing in personal data protection (DPD) and a data protection officer (DPO) and to inform A05 of such DPD and DPO</p>



Action required
<p>To develop:</p> <ul style="list-style-type: none"> • Data breach response procedure/policy • Template of written confirmation of the occurrence of breach • Template of data breach notification
<p>To appoint DPO/DPD in case of processing sensitive personal data</p>

Roadmap for compliance



Administrative penalty for violation

No official sanction decree in place yet. In general, as prescribed by Vietnam PDPD, sanctions applicable may include: disciplinary measures, administrative penalties and criminal prosecution

Summary of the administrative penalty types under the latest [DRAFT Decree on Penalties in Cybersecurity](#)

Monetary fine

- ▶ Basic: Ranging from VND40 mil to VND200 mil (applicable to organizations/legal entities)
- ▶ For some violations, subject to the severity of the violation, the company can be fined up to **2-5 times the basic monetary fine** or even be fined **3%-5% of the total revenue** in Vietnam

Additional measures

- ▶ Suspension of the right to use business licenses for industries requiring personal data collection from 1 to 3 months
- ▶ Confiscate evidence and means of processing personal data for violations
- ▶ Expel from the territory of the Socialist Republic of Vietnam

Remedial measures

- ▶ Public apology on the mass media
- ▶ Being forced to stop processing personal data from 1 month to 3
- ▶ Forced destruction or deletion to the point where personal data cannot be restored
- ▶ Forced return or forced return of illegal profits obtained from committing violations

Challenges from a legal perspective

What aspects of compliance might businesses struggle with?

1. Inability to accurately identify and understand the overall landscape of personal data processing activities

- ▶ Lack of understanding makes it difficult to create a data inventory or data flow mapping

2. Complication of ensuring data subjects grant consent and be notified before the processing

- ▶ Each method of collection requires an appropriate consent obtainment mechanism that is quick, efficient, and also in compliance with the law.

3. The development or enhancement of an internal data protection framework can be a demanding requirement

- ▶ Vagueness for the type or content of the internal framework required to ensure compliance
- ▶ Lack the necessary resources to prepare or review all internal policies related to personal data protection.

4. Effectiveness of the Data Protection Officer's (DPO) role

- ▶ Shortage of skillful personnel with expertise in personal data protection to take on the DPO role
- ▶ Financial burden of recruiting for this position, poses a significant challenge in finding appropriate personnel.

5. Notably deficient level of employee awareness

- ▶ Many if not most employees currently do not have an in-depth understanding of the personal data protection landscape

6. It is imperative for enterprises to coordinate with third parties (partners) to ensure the protection of personal data

- ▶ Renegotiating and reaching personal data processing agreements with current and potential partners. This can take time and impact business cooperation opportunities
- ▶ Difficulties in creating effective coordination mechanisms between parties when a personal data breach occurs

A comprehensive legal and technological solution to the compliance challenges

Framework enhancement

- ▶ Enhancement of framework may comprise of: (i) Consent and notification forms; (ii) Mechanisms, processes, and forms to enable the exercise of data subjects' rights; (iii) Internal data management mechanism such as data retention, data processing activities for effective coordination and implementation; (iv) Breach response policy; (v) Due diligence process and contractual arrangement with third parties
- ▶ Consistency with other internal policy documents
- ▶ Adjustments of global policies
- ▶ Third party management

Personnel

- ▶ Periodic training sessions
- ▶ Tailoring for different groups of subjects is required
- ▶ The DPO/DPD appointment be formalized in written form, clearly stating the rights and obligations of these individuals.

Technology

- ▶ Technology plays a vital role in the integration of the framework to operation
- ▶ The coordination with the internal information technology (IT) department and sometimes third-party service providers is required.

EY Service engaged
related to data privacy

Service offering (1/3)

No.	Services Description	Scope of Work
1	Data privacy compliance healthcheck	<p>Under this assignment, our tasks will include:</p> <ul style="list-style-type: none"> • Review the provided information and documents to observe any non-compliances of the Company in relation to personal data protection; • Assess the maturity level of current process, procedures, legal framework and operation in relation to the PDPD; • Prepare a written report (“Report”) in English covering the following areas: <ol style="list-style-type: none"> i. Summary of data processing activities; ii. Non-compliances of the Company against regulations on personal data protection; iii. Legal implications/ legal risks the Company may subject to under Vietnamese law; iv. Recommendations on appropriate legal actions to rectify the non-compliances if possible; v. Recommendations or a list of initiatives on operations, processes, procedures, solutions to fulfill requirements of personal data protection. <p>Note: EY will attend up to 02 (two) rounds of discussion on legal matters with the Company pertaining to our first draft of Report.</p>
2	Drafting/Reviewing personal data protection documents	<p>Draft/review personal data protection term in necessary documents pertaining to the personal data protection activities of the Company in accordance with the laws of Vietnam;</p> <ul style="list-style-type: none"> • Obtain relevant documents and information to be provided by the Company; • Review and inputting the personal data protection terms in the following documents: <ul style="list-style-type: none"> • Definite-term labour contract (Bilingual – Vietnamese and English); • Indefinite-term labour contract (Bilingual – Vietnamese and English); and • Internal labour regulations (both Vietnamese and English versions); • Prepare the following documents: <ul style="list-style-type: none"> • Consent form and notification on data processing to employees and/or candidates (Bilingual – Vietnamese and English); and • Personal data protection manual/guideline/policy applicable to employees and/or candidates (both Vietnamese and English versions); • Attend up to 02 (two) rounds of follow-up questions or comments from the Company pertaining to the first draft/first reviewed version of documents; • Finalize the documents based on the Company's comments

Service offering (2/3)

No.	Services Description	Scope of Work
3	Preparation of data processing impact assessment; and Preparation of cross-border data transfer impact assessment	<p>Under these two assignments, we will:</p> <ul style="list-style-type: none"> • Assist in drafting necessary standard impact assessment in Vietnamese based on documents and information provided by the Company in accordance with Vietnam regulations; • Attend up to two rounds of follow-up questions or comments from the Company pertaining to the draft version of documents; • Finalize the documents based on the Company's comments. <p>Note: EY will not assist in submitting the assessment reports and applications to competent authority.</p>
4	Breach management	<ul style="list-style-type: none"> • Prepare (i) a procedure for breach handling and draft (ii) a breach notification form in Vietnamese. • Attend up to 02 (two) rounds of follow-up questions or comments from the Company pertaining to the first draft version of documents. • Finalize the documents based on the Company's comments.
5	Third-party management	<p>EY will assist the Company with the following tasks:</p> <ul style="list-style-type: none"> • Reviewing the personal data protection terms in the personal data processing contracts with third party, including: Workpermit agreement; Payroll service contract; tour service agreement; insurance service agreement; etc. (both Vietnamese and English versions). • Identifying material non-compliance areas against prevailing regulations on personal data protection under Vietnamese law and corresponding legal implications/ legal risks; • Inputting the personal data protection terms (if not available yet); • Attending up to 02 (two) rounds of discussion and/or clarification with the Company pertaining to our first delivery of the documents; • Finalizing the documents based on the Company's comments.

Service offering (3/3)

No.	Services Description	Scope of Work
7	Personal data protection awareness training	<ul style="list-style-type: none">• Prepare a comprehensive legal slide deck, discussing the key topics of PDPD (including principle, subjects and definition, groups of regulated subjects, consent requirement and exception, prior notice requirement, data subject rights, data protection impact assessment, cross-border personal, data transfer impact assessment, personal data protection authority, special cases of processing, protection measures, obligation of personal data controller/controller-processor/processor) and required actions and best practices from a legal perspective;• Setup meetings with the Company for conducting personal data protection awareness training; and• Conduct training session with the Company in Vietnamese <p>• Beyond the scope set forth in Section 1-7 above, any other legal supports in working with the Company's representatives upon request in connection with personal data protection and in the operational course of the Company will be considered ongoing support on data privacy matters.</p>
8	Ongoing support in data privacy matters	<ul style="list-style-type: none">• Under this scope we will:<ul style="list-style-type: none">• Attend meetings or discussions with the Company regarding any legal issues in relation to personal data protection during the operation of the Company.• Provide comments via emails, calls on matters incurred from legal perspective upon the request of the Company, and recommend the appropriate courses of action.• Provide legal advice on data privacy issues, if any.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2024 EY Law Vietnam Limited Liability Company. All Rights Reserved.

APAC No.16230201
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/en_vn





BEST PRACTICE IN SAFEGUARDING CUSTOMER PERSONAL DATA



WHY IS YOUR IT SECURITY CRITICAL?



Data Breaches in Europe

Company Name	Country	Industry Sector	Cause of Fine	Amount of Fine (USD)
Google	France	Technology	Lack of transparency and consent for personalized ads	\$57,000,000
Google	France	Technology	Failure to provide clear and comprehensive privacy information	\$120,000
H&M	Germany	Retail	Surveillance of employees	\$41,000,000
Marriott International	UK	Hospitality	Failure to protect personal data	\$23,900,000
British Airways	UK	Transportation	Failure to protect personal data	\$22,000,000
Vodafone	Germany	Telecommunications	Unauthorized collection of personal data	\$11,000,000
TIM	Italy	Telecommunications	Unsolicited telemarketing	\$29,000,000
Wind Tre	Italy	Telecommunications	Unsolicited telemarketing	\$18,000,000
Google	UK	Technology	Failure to obtain consent for personalized ads	\$57,000,000
Google	Ireland	Technology	Failure to obtain consent for personalized ads	\$57,000,000
Uber	UK	Transportation	Failure to protect personal data	\$491,000
AOK Baden-Württemberg	Germany	Healthcare	Insufficient technical and organizational measures	\$1,800,000
Eni Gas e Luce	Italy	Energy	Unsolicited telemarketing	\$11,000,000
Google	Belgium	Technology	Failure to comply with right to be forgotten requests	\$680,000
Notebooksbilliger.de	Germany	Retail	Insufficient technical and organizational measures	\$12,500,000
Iliad	France	Telecommunications	Failure to obtain valid consent for advertising cookies	\$5,000,000
Deutsche Wohnen	Germany	Real Estate	Retention of personal data beyond necessary period	\$15,000,000
Austrian Post	Austria	Postal Services	Unauthorized use of personal data for direct marketing	\$19,000,000
Google Ireland Limited	Ireland	Technology	Failure to provide sufficient information to data subjects	\$1,650,000
Deutsche Bank	Germany	Finance	Failure to prevent money laundering	\$16,000,000

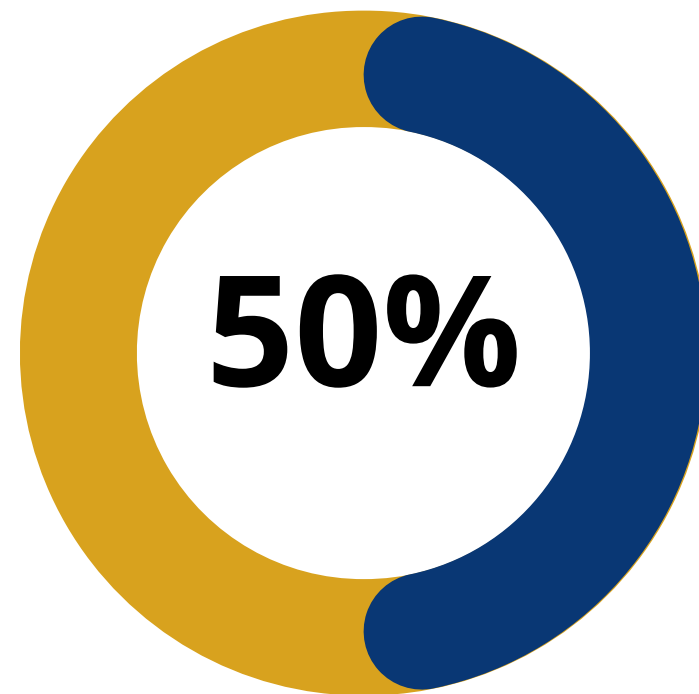
Data Breaches in S'Pore

Industry Sector	Company Name	Cause of Fine	Reason for Failing	Amount of Fine (USD)
Healthcare	SingHealth	Failure to provide notification of breach	IT Security related	\$185,000
Healthcare	IHiS	Failure to secure patient data	IT Security related	\$555,000
Telecommunications	StarHub	Unauthorized disclosure of personal data	Legal issue	\$155,000
Telecommunications	Singtel	Unauthorized disclosure of personal data	Legal issue	\$18,500
Logistics	Ninja Logistics	Failure to secure customer data	IT Security related	\$67,500
Logistics	Best Logistics	Failure to secure employee data	IT Security related	\$16,700
Ride-hailing	Grab	Failure to inform customers about policy	Process oriented	\$7,400
Technology	Ericsson	Failure to secure employee data	IT Security related	\$8,100

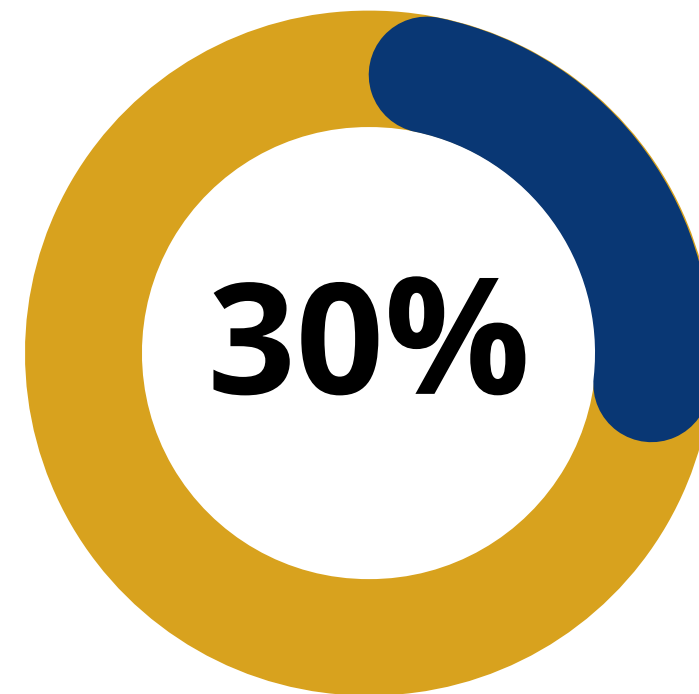
DID YOU KNOW?

Approximate content of the PDPA law

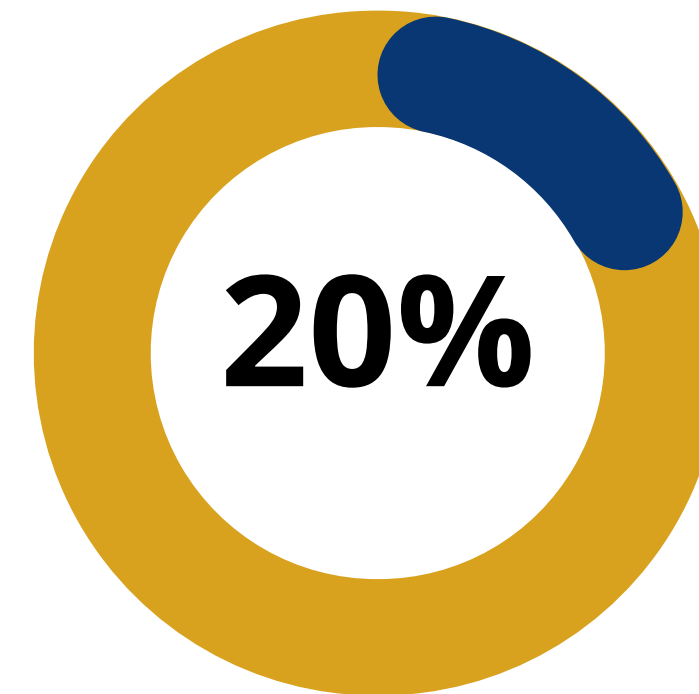
IT Security



Awareness



Legal





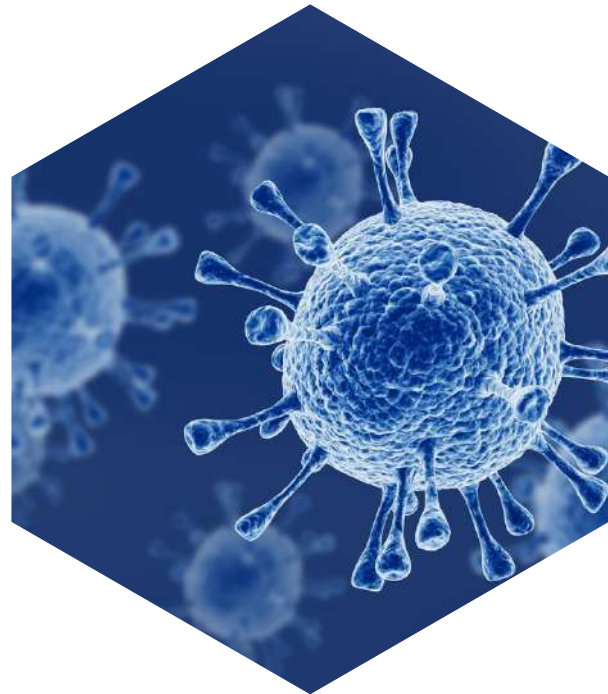
MALWARE EVOLUTIO

N

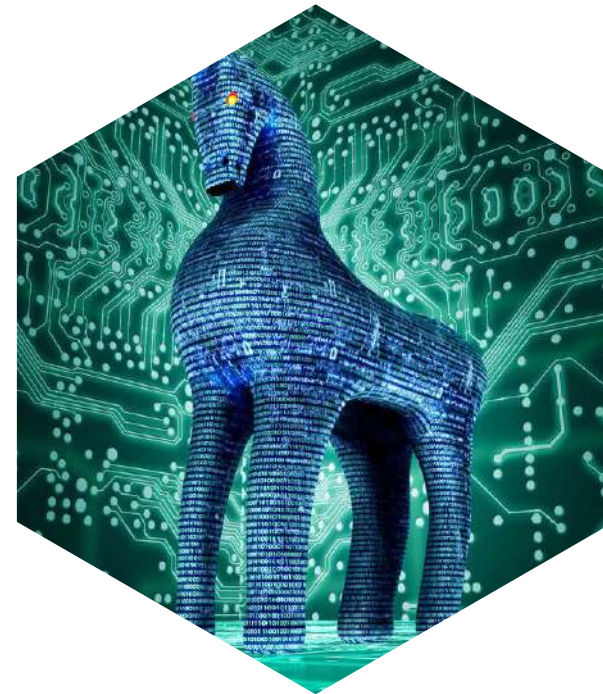


TRADITIONA

L



Virus



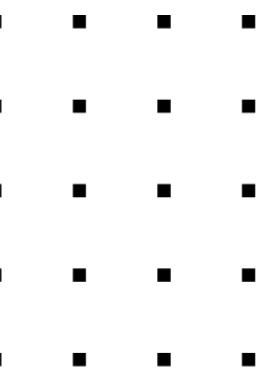
Trojan



Worm



Phishing



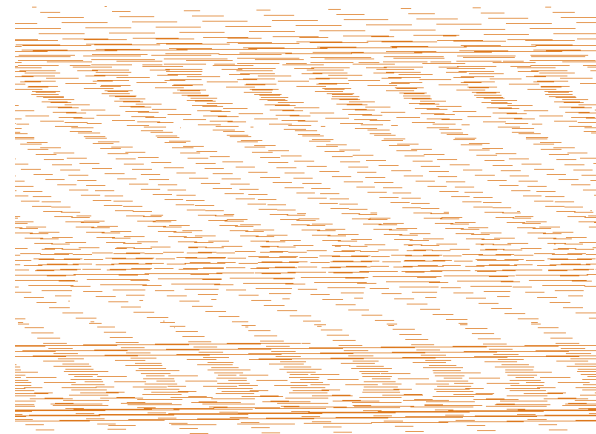
RANSOMWAR

E

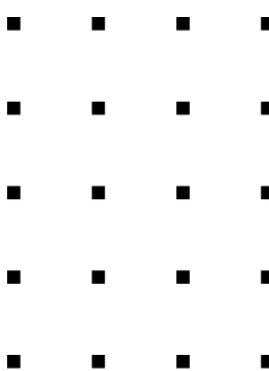
2 step infection



Phishing



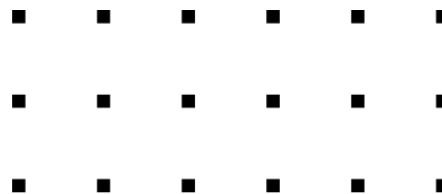
- Call for additional code
- Execute Disk Encryption
- Erase local visible backup
- Propose sample test decrypt
- Collect ransom



Large companies are now more protected

- Prepared with backup Strategy
 - Damage limited to downtime
 - Server mirroring
 - Aware and trained IT Team

Need to refocus on other targets





SMEs with high Profile

Audit Companies

Accounting Firms

Lawyers

IT Security Companies

Health Industry

Medical Equipment

Software Industry

Food Companies

And..... YOURS!



SME

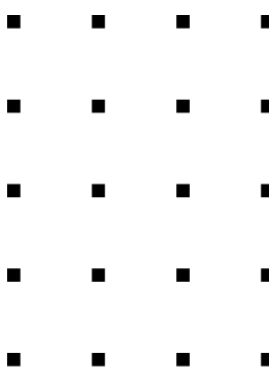


BUILDING LEVERAGE

Using PDPA Compliance Requirements to trap new victims

- High Fine - Up to 5,000,000 THB
- Jail term
- Potential civil case
- Time pressure to react (72h)
- Unprepared victims

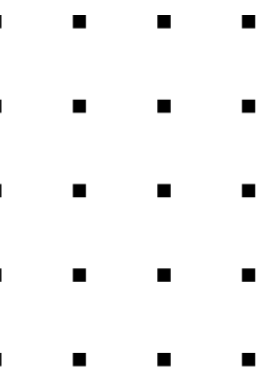
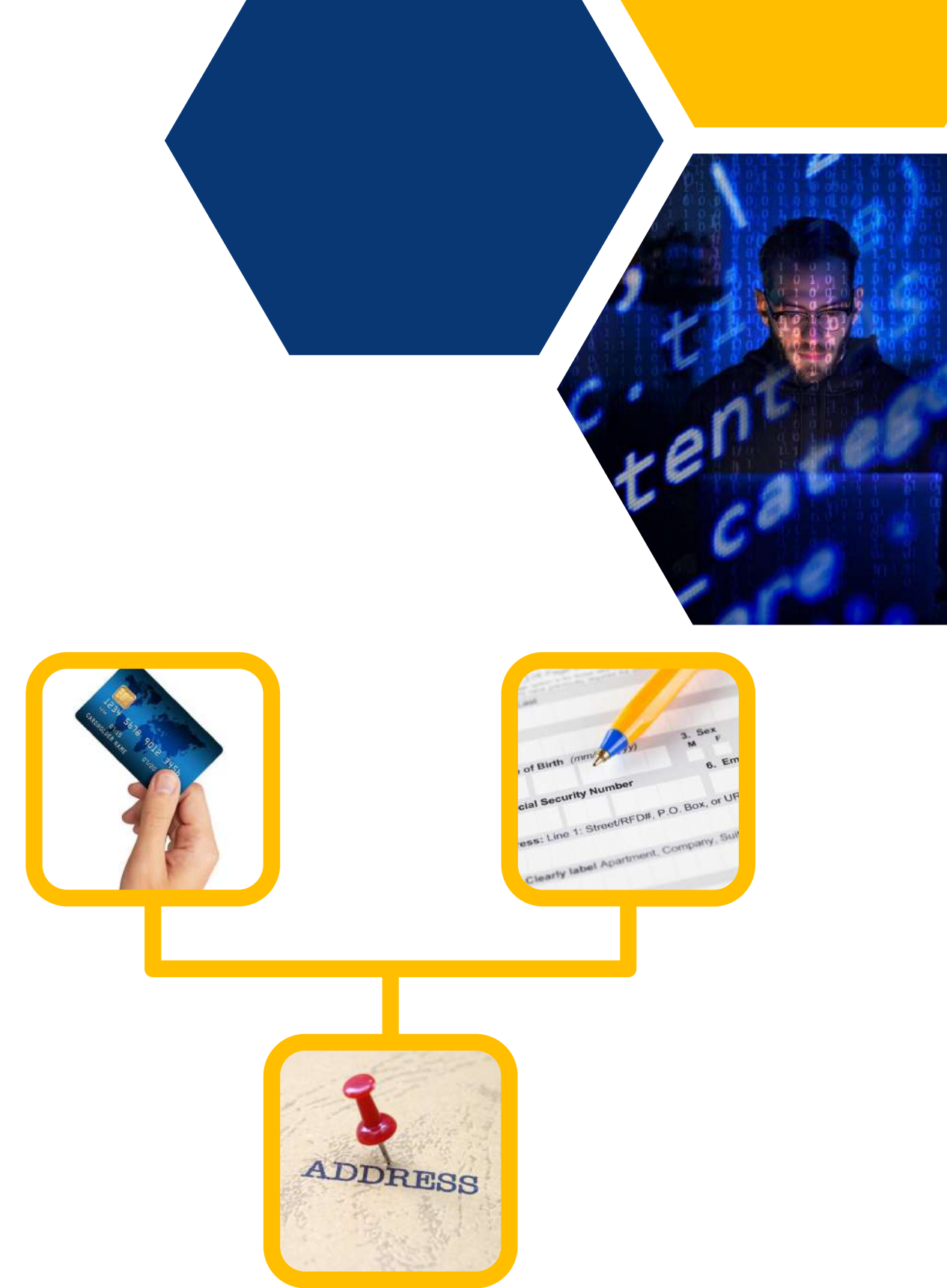
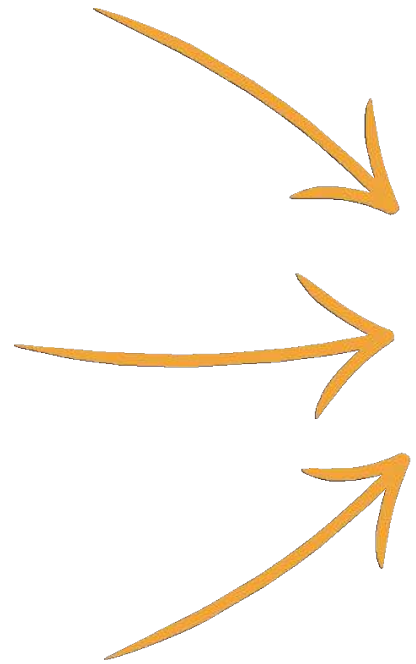
- Clear processes missing
- Untrained persons in charge
- General requests to the wrong target



CASE 1

A white hacker used a fake gmail address to request information about his GF

- Created a Gmail account in her name
- Sent to 150 companies
- Received 80 confirmations of data
- 37 complied with sending
 - CC details, Bank info
 - Social security numbers
 - Full address, etc...



How easy?

Spot the Difference?

maybank2u.com is not the same as
maybank2u.com

citibank.com is not the same as
citibank.com

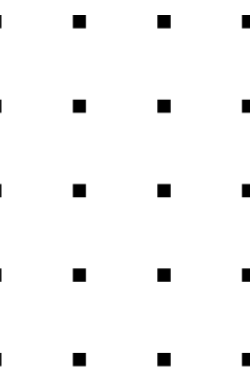
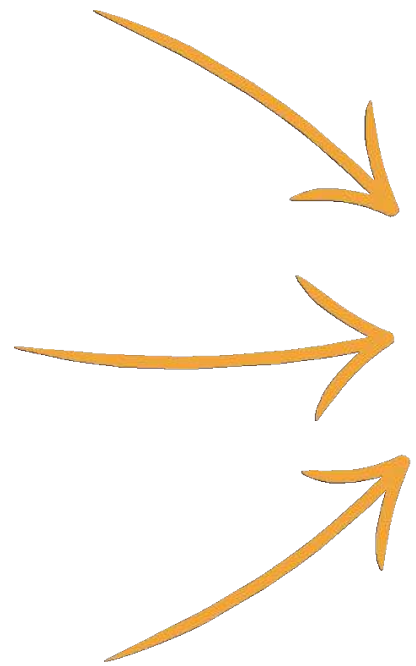
(the first one is correct, the second one
is from hackers)



CASE 2

Brute force on a music sharing basic account with a weak password

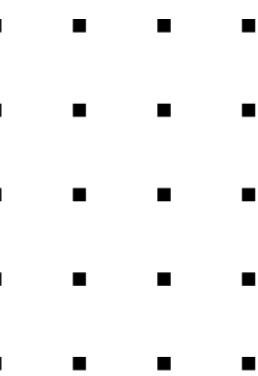
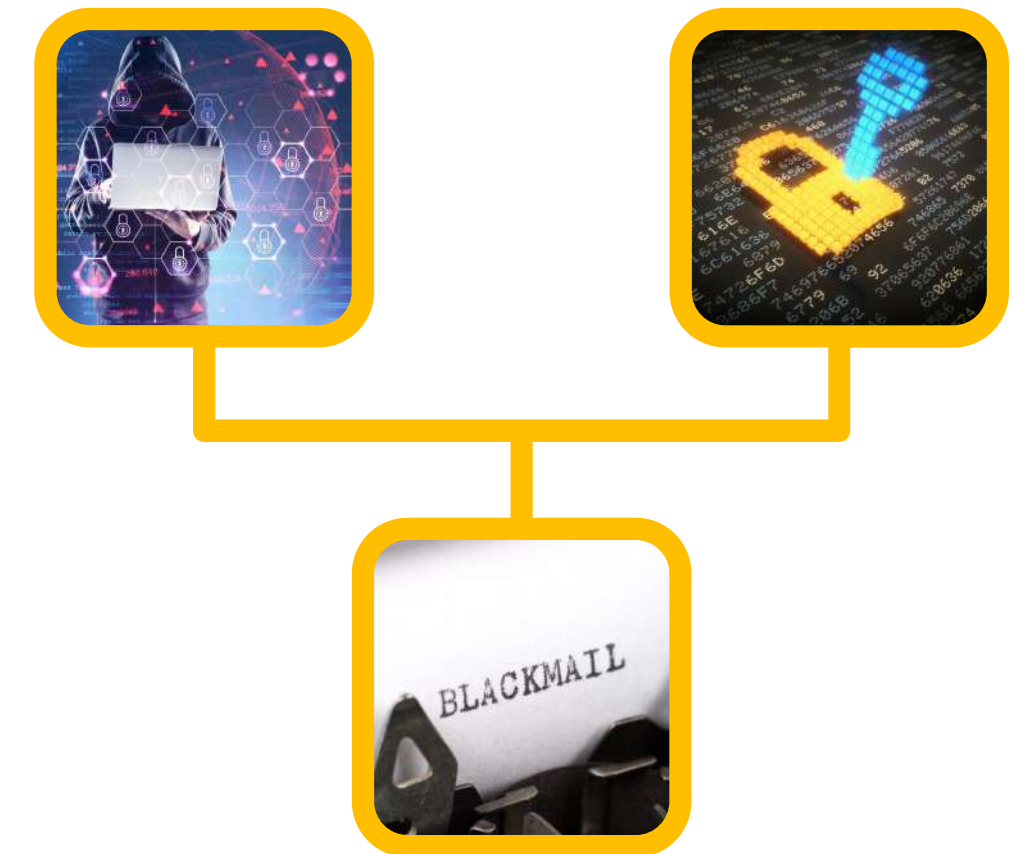
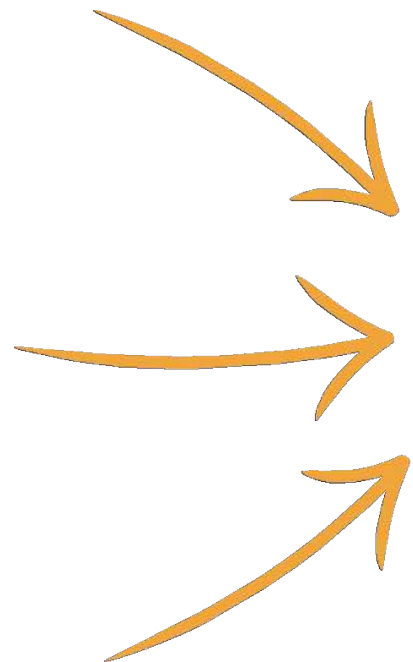
- Weak protection (data not critical)
- Hacker brute forces the password
- Escalate to change the email
- Request to verify all details
- Received immediately
 - CC details, Bank info
 - Family composition
 - Full address, etc...



CASE 3 Reversed Ransomware

After encryption a copy of the data was ex-filtered to the hacker site

- Attack with a phishing exploit – link
- Installed a worm on the network
- Propagation through the Network
- Encryption of Data, removal of Backup
- Ex-filtering of data to a hacker site
- Removal of data, only encrypted stays
- Submit a request for ransomware
- Double threat with personal data exposed on the web
- Very high fine + civil court + reputation



How to protect yourself?



Know your position



Train your people - ALL of them



Reinforce your IT Security



Document your efforts



Prepare: data segregation, Silos



Monitor



STEP BY STEP PROTECTION

A down to earth practical approach

Gap Assessment - Audit

Document processes & inventory

Set up Policies

Check 3rd Party compliance

Deploy Technology (\$)

Train people: IT & PDPA Awareness

DOCUMENT YOUR EFFORTS



Essential Pre-requisite

IT Security Audit

What is an IT Security Audit?

It is a **comprehensive assessment** of your organization's security posture and **IT Infrastructure**. Conducting an IT security audit helps organizations **find and assess the vulnerabilities** existing within their IT networks, connected devices, and applications.



IT Awareness Training

Internet Driving License

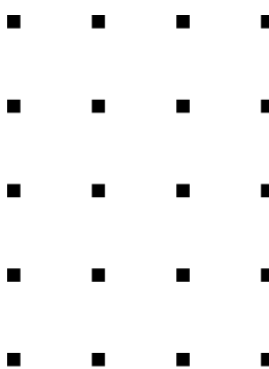
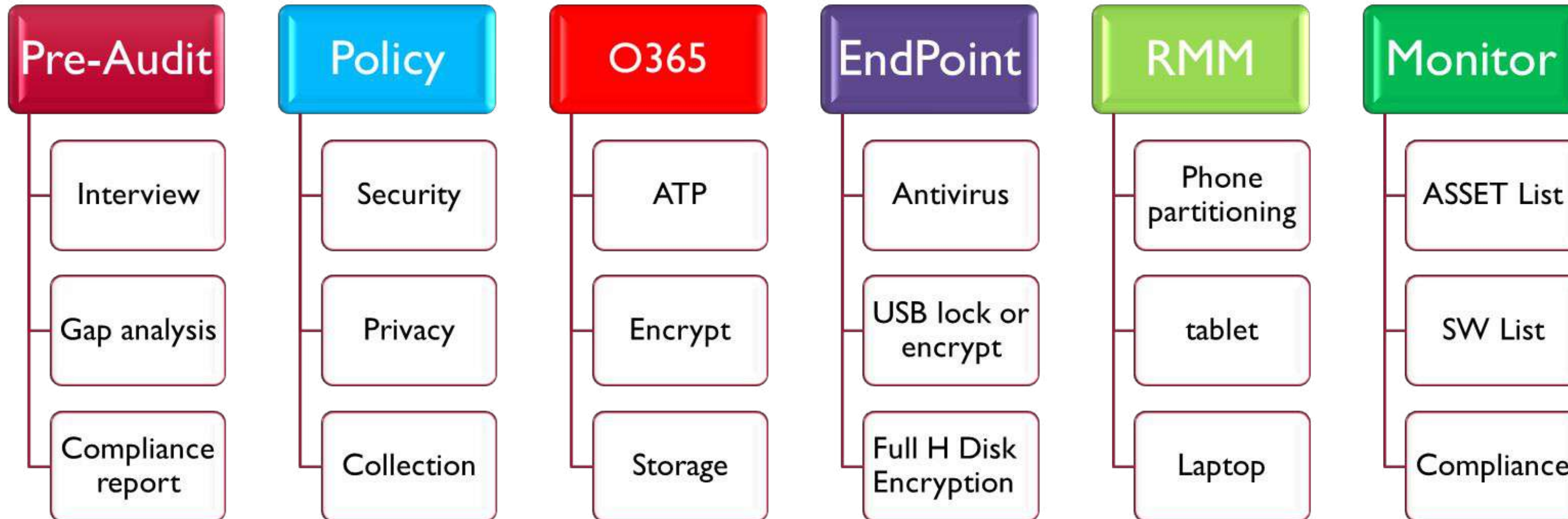
Nowadays, any admin staff, any sales person any manager is provided with a **sophisticated computer and high-speed internet access.**

Still, there is **little or no training** given in handling such a powerful tool.

It's like **giving an F1 Car to a new driver!**



In a Nutshell





GET IN TOUCH

SafeComs Network Security Consulting Co.,Ltd



Eddy Bellavoine

Chief Commercial Officer (CCO)



EMAIL ADDRESS

eddy@safecom.com



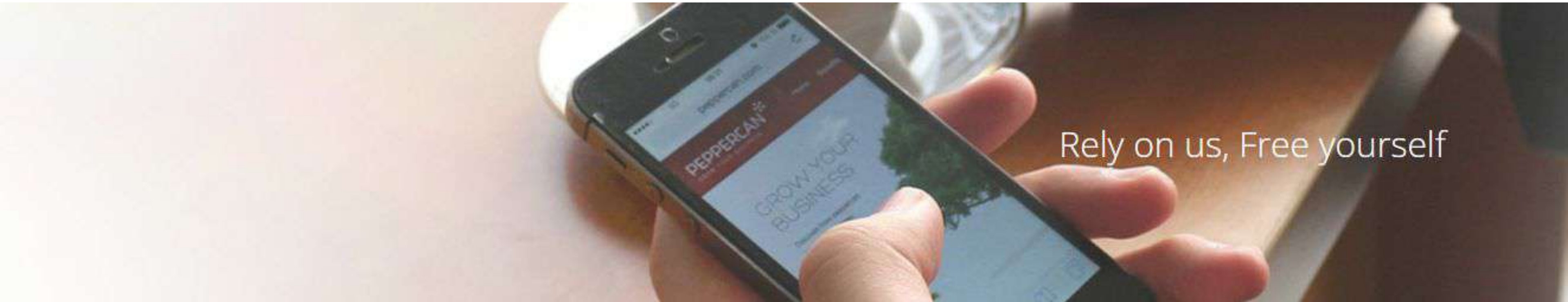
PHONE NUMBER

+66 89 486 8611



WEBSITE

www.safecom.com.th



Rely on us, Free yourself

Adopting GuardTech To Protect Your Data And IT Security

It is a **creative and innovative** remote monitoring and maintenance system.

It's a cutting-edge service to ensure your **Peace of Mind, and strengthen your data protection!**

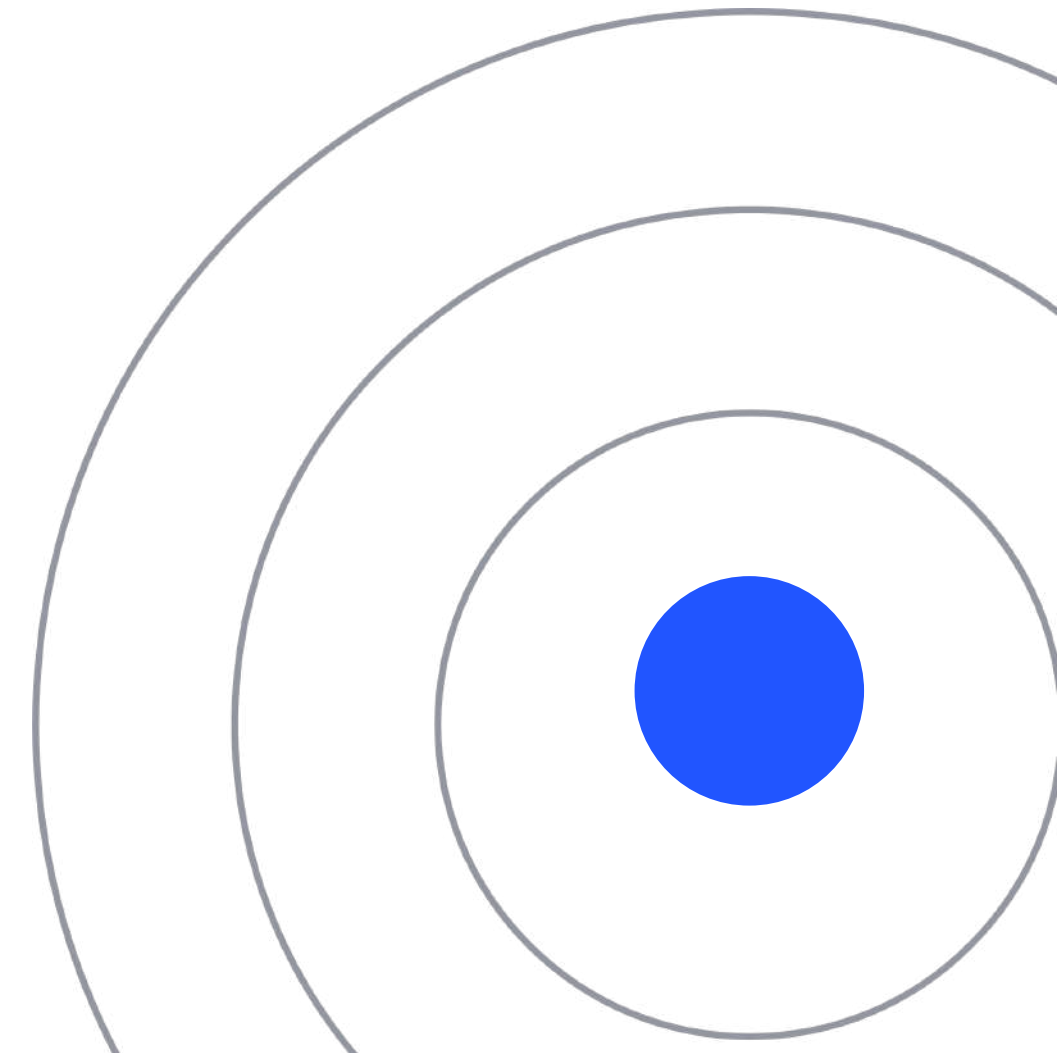
AHT Tech



SafeComs



GuardTech & IT Security Management



Why? ●

- 1** Customized solution for over 10+ years, boosting IT security and efficiency.
- 2** Technology transforming our operations.
- 3** COVID-19 led to a challenge: engineers couldn't visit clients.
- 4** Adopted GuardTech, in response to new challenges.

Why? ●

5

No on-site visits needed.

6

Manages multiple endpoints and clients simultaneously.

7

Optimize resources and service delivery.

8

We DO NOT access your data

GuardTech ●



- ✔ Remote, proactive monitoring
- ✔ Issue detection and reporting
- ✔ Issue resolution from a remote location
- ✔ IT Management tools accessible

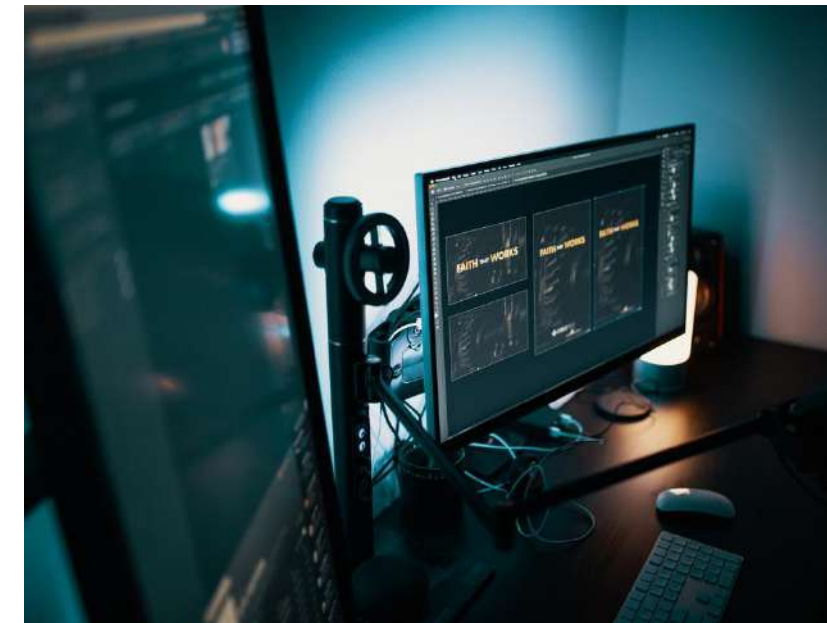
Which



device?



Server



Desktop



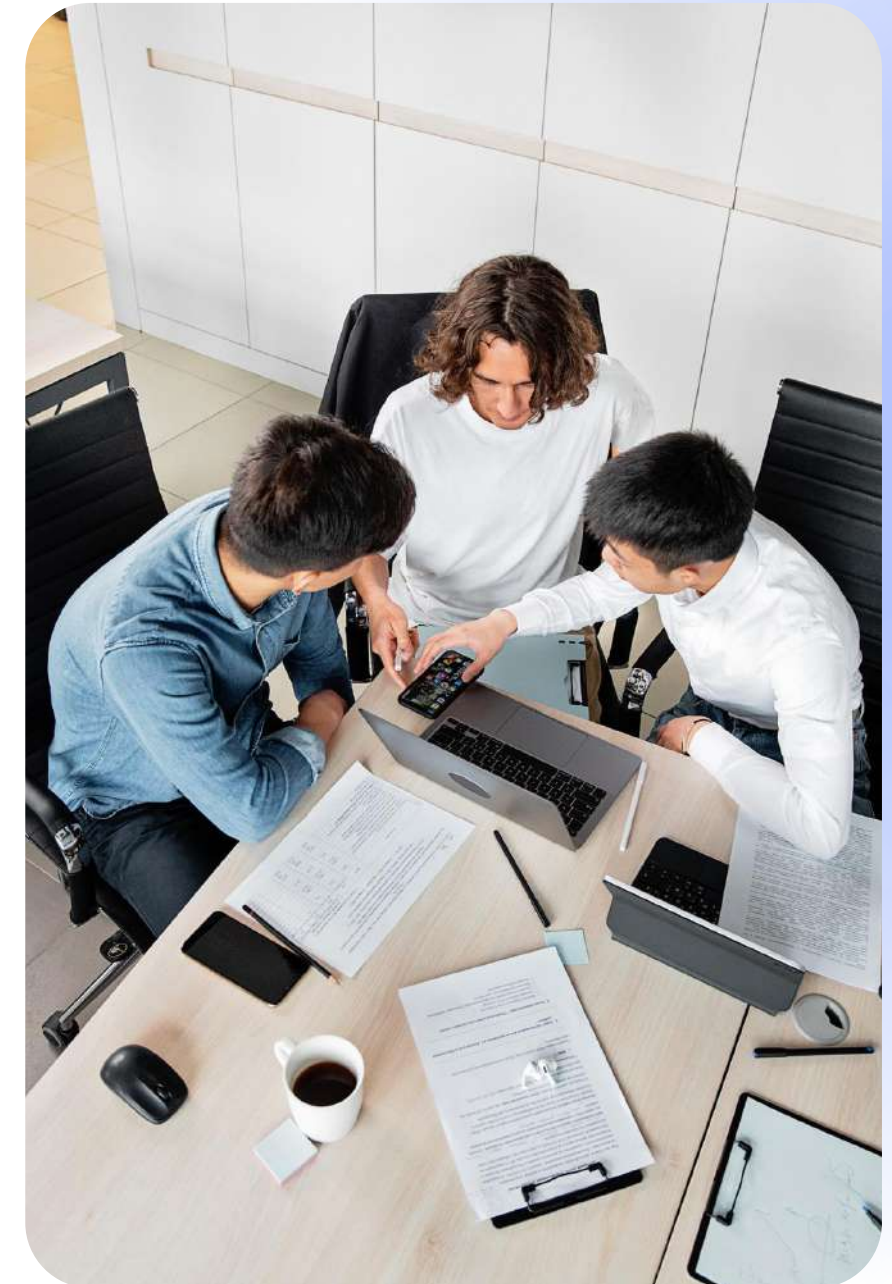
Laptops



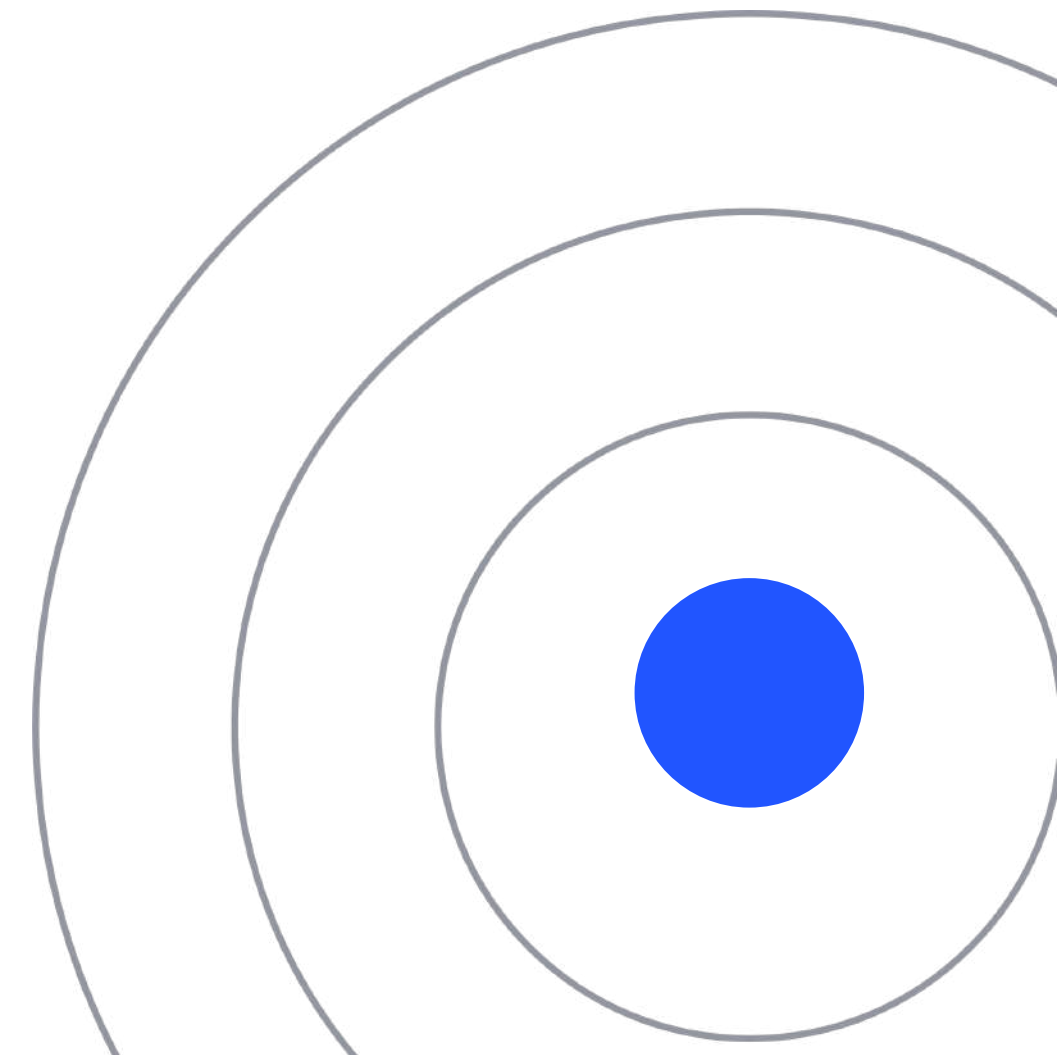
Windows,
Linux & Mac

Attribute ●

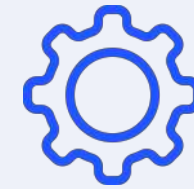
- S**
- ✔ Remote agents without VPN.
 - ✔ Perform tasks with clients offline.
 - ✔ Fix issues without work disruption.
 - ✔ Engineers use agents or consoles.



Features & Benefits



Comprehensive Remote IT Management ●



Feature

Manages and monitors IT infrastructure entirely remotely, leveraging advanced technology for oversight.



Benefit

Eliminates the need for a physical IT presence, leading to significant cost savings and less intrusiveness in daily operations.

Proactive Issue

Detection & Resolution



Feature

Utilizes sophisticated algorithms to predict and address IT issues before they impact business operations.



Benefit

Dramatically reduces system downtime, enhancing productivity and safeguarding against potential revenue losses.

Robust Cybersecurity Measures ●



Feature

Implements top-tier security protocols to defend against cyber threats, including real-time monitoring and regular updates.



Benefit

Strengthens data protection, ensuring compliance with privacy regulations and maintaining customer trust.

Optimized Resource Utilization ●



Feature

Efficiently allocates and manages IT resources, ensuring optimal hardware and software performance.



Benefit

Increases overall business efficiency and performance, allowing for more focused resource allocation in other areas.

Flexible Scalability ●



Feature

Designed to effortlessly scale with your business, accommodating changes in size and scope.



Benefit

Facilitates seamless growth without IT constraints, ensuring that IT infrastructure evolves with the company.

Decreased Maintenance Needs ●



Feature

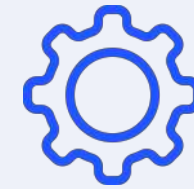
Reduces unforeseen IT expenses through preventative maintenance and efficient management.



Benefit

Facilitates seamless growth without IT constraints, ensuring that IT infrastructure evolves with the company.

Stable and Reliable IT Environment ●



Feature

Maintains a consistent and high-performing IT infrastructure.



Benefit

Increases overall business efficiency and performance, allowing for more focused resource allocation in other areas.

What is GuardTech included? ●



Alerts: Uptime, storage, connectivity, backup, security (virus and patches)



Antivirus definition updates



Patch Management



Remote support



Defragmentation of hard drives (when applies)



Software Installation, repair, removal



Inventory always up to date



Set up routine, scheduled maintenance tasks, and prevention of problems.



Software and Hardware audits



Automated process with remediation.

Benefits

1

Quick resolution: No waiting for onsite visits.

2

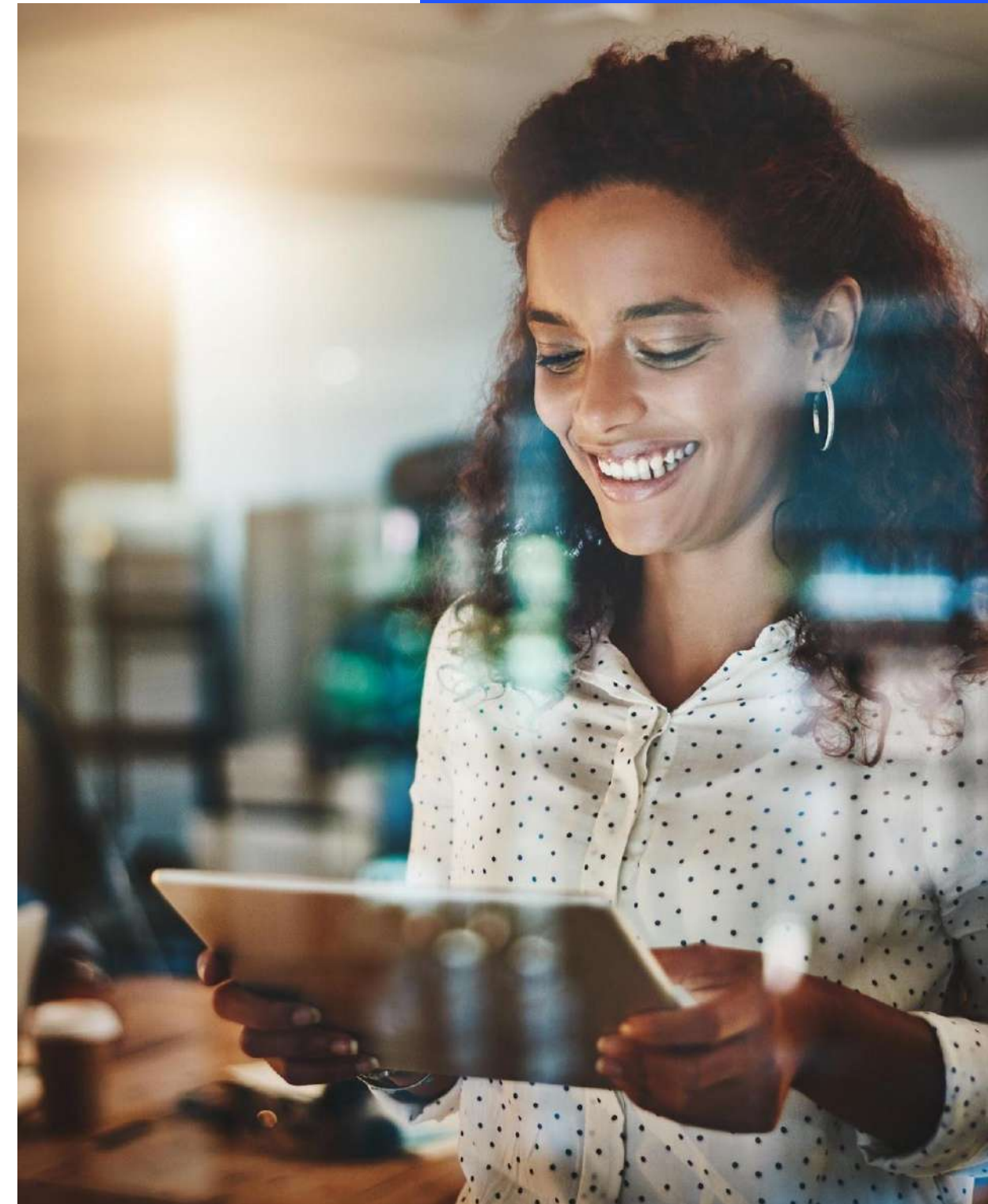
Enhanced security: Active management and monitoring.

3

Increased stability: Standardized environment, less downtime, more productivity.

4

Proactive Monitoring: Real-time alerts with GuardTech.



Benefits ●

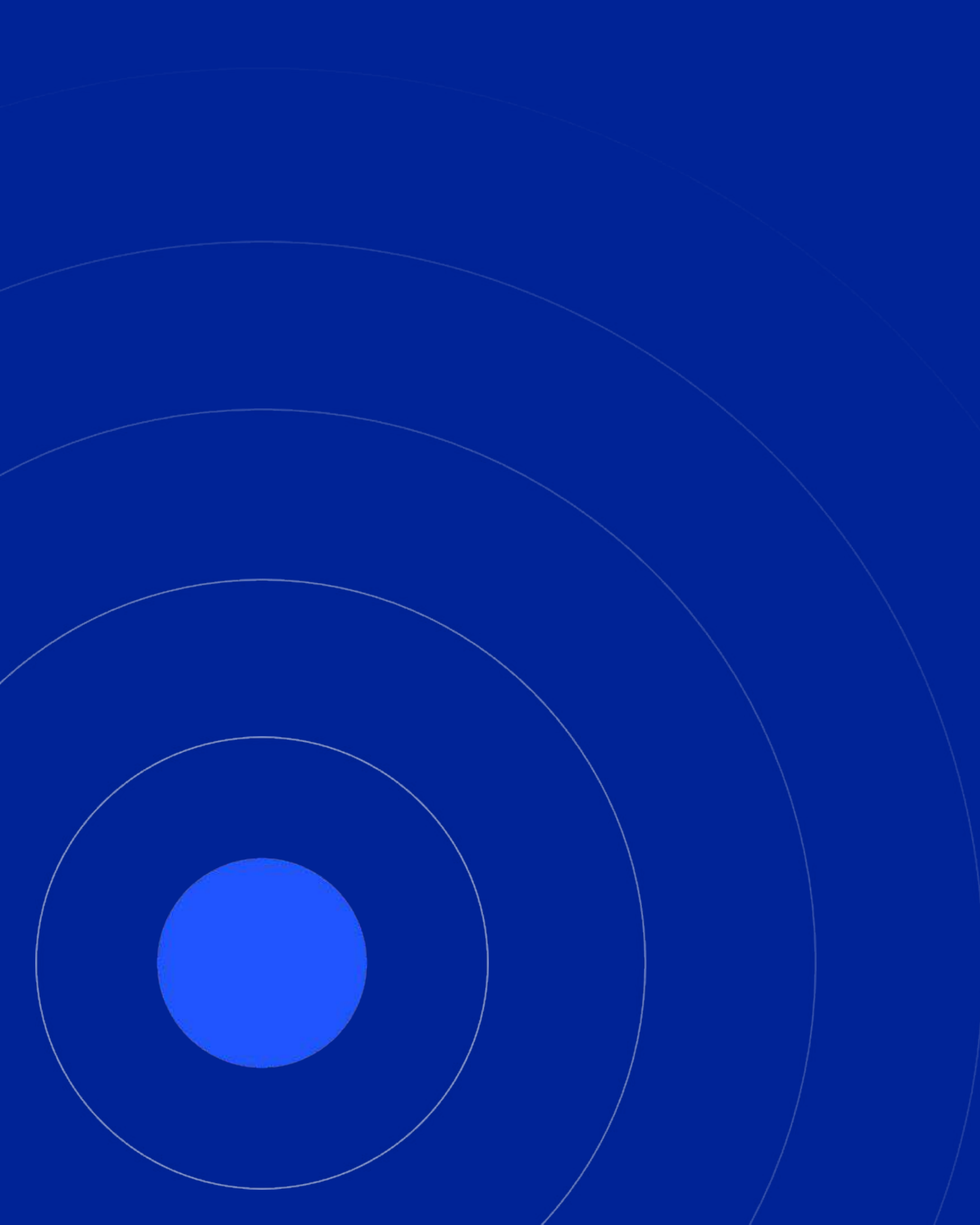
5 Minimized Downtime: Early issue detection.

6 Improved Security: Enhanced data and network protection.

7 Reduced Maintenance: Automated routine tasks, resource-efficient.

8 Increased Productivity: Multi-monitor support for effective multitasking.





ABOUT AHT TECH

ABOUT AHT TECH

16+
Years of experience

500+
Employees

1000+
Clients

5000+
Projects

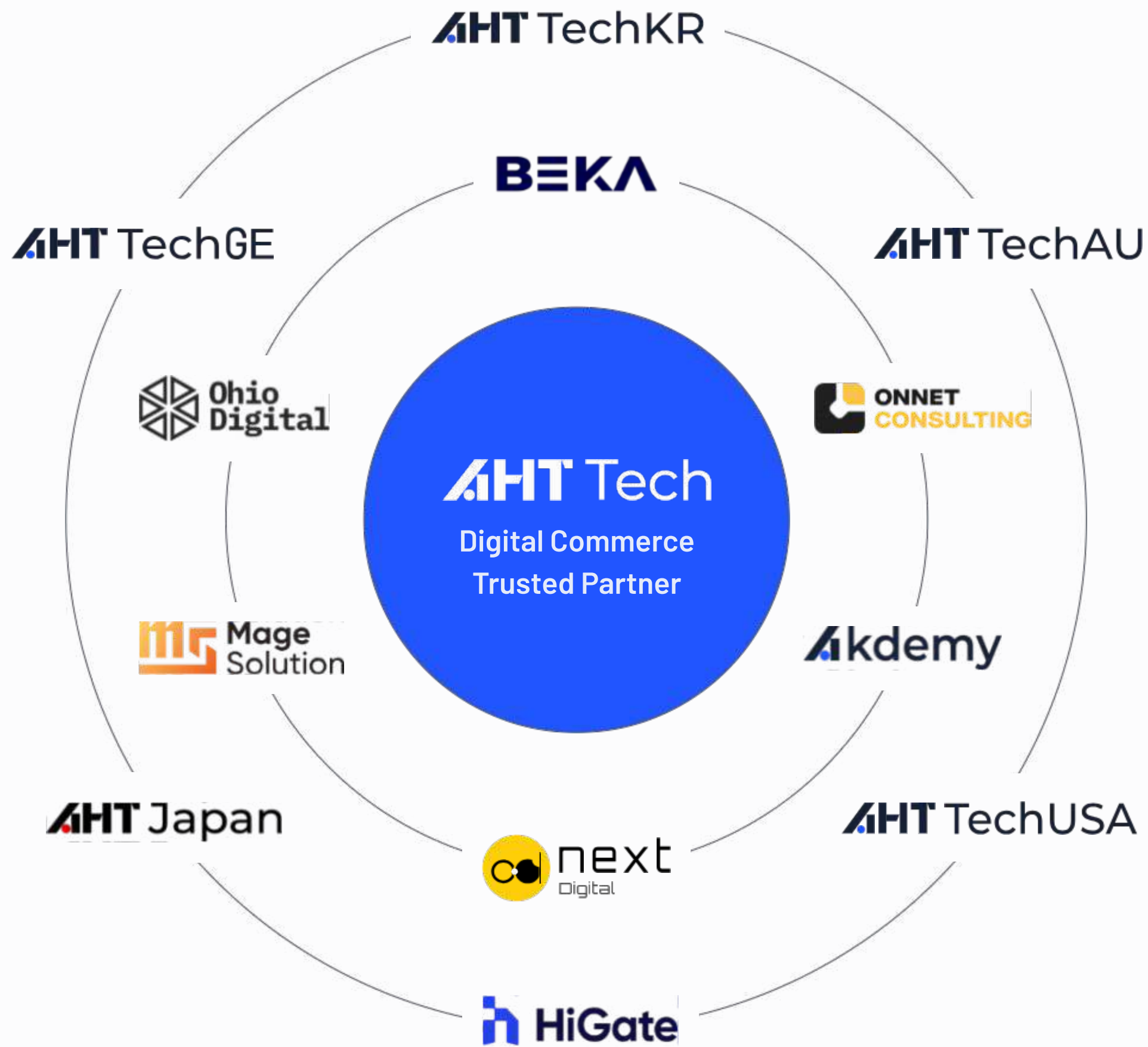
Headquarter
Hanoi, Vietnam



Established
2007

Awards & Certificates





Business Network in 9 countries



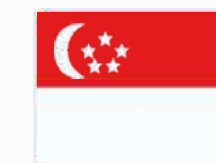
Australia



Germany



United States



Singapore



Japan



Korea



Vietnam



Malaysia



Thailand



OUR SOLUTIONS & SERVICES



ERP

We are the premier ERP consulting company with a full range of ERP consulting services & solutions to power your business to achieve higher performance:

- Odoo ERP
- Acumatica
- Oracle Netsuite
- Open Educate

**CLOUD DATA PLATFORM
& CYBER SECURITY**

ECOMMERCE



OUR SOLUTIONS & SERVICES

ERP



CLOUD DATA PLATFORM & CYBER SECURITY

We help you mitigate effort and control risk when moving to cloud with our services of cloud data platform and cyber security

- Snowflake
- Data bricks
- Tableau
- Cyber Security

ECOMMERCE



OUR SOLUTIONS & SERVICES

ERP

CLOUD DATA PLATFORM &
CYBER SECURITY



ECOMMERCE

We provide full range of eCommerce solutions: consulting, development, optimization, implementation and maintenance:

- Magento
- Shopify Plus
- Commerce tools
- Bigcommerce

OUR SKILLS & TECHNOLOGY

COPYRIGHT AHT TECH 2024

Consulting and implementation capabilities

- Web/ Mobile app development
- Custom software development
- AI & Machine Learning, The IoT
- AR, VR
- The Blockchain
- Data Warehouse & Data Lake
- Cloud Computing
- DevOps

500+ Software engineers

**CUTTING-EDGE SOLUTIONS
& TECHNOLOGIES**

Platforms Driven & Solution architect capabilities

- Cyber Security 
- ERP    
- DATA   

100+ Technology & Industrial Experts

**GLOBALIZED
STANDARD QUALITY**

Business domain knowledge

- Retails& Ecommerce
- Manufacturing
- BFSI
- Education
- Professional services
- Wholesales & Distribution
- IT & Telecom
- Logistics
- Healthcare
- Construction
- Agriculture

60+ Platforms certificates

**IN-DEPTH, CUSTOMIZED AND
OPTIMIZED SOLUTIONS**




OUR APPROACH METHODOLOGY

COPYRIGHT AHT TECH 2024

How we approach to deliver digital commerce solutions & services

DIGITAL LEAN - OUR APPROACH METHODOLOGY


Big Picture Thinking



Customized Business-domain
Solution Mindset



Lean Implementation, On-time Delivery
& Fast Scalability

Requirement
Analysis

Test-Driven development with
sandbox models, optimize &
evaluate ROI, SWOT

Solutions Consulting
& Technology
Recommendations

Monitoring, support
& Maintenance

Tailored Tech
Development

OUR CORE COMPANY CULTURE PHILOSOPHY

OUR CORE VALUES

Customer-Centric Solution | Always People First | Innovative Technology

OUR MANAGEMENT PHILOSOPHY

Integrity | Ascendancy | Reliability | Positivity | Pioneer



BRANDS WE WORK WITH

BFSI



MANUFACTURING



RETAILS & E-COMMERCE



AMORE PACIFIC

TOKYO LIFE

WHOLESALE & DISTRIBUTION

plantronics



TELCO & OTHERS

mobifone

viettel



kenanga



Academy Xⁱ



CONTACT US

AHT Tech JSC

HEADQUARTERS

8F, MITEC Building, Duong Dinh Nghe Street,
Yen Hoa, Cau Giay, Hanoi

E-MAIL

info@arrowwhitech.com

PHONE

(+84) 24 3795 5813

WEBSITE

www.arrowwhitech.com





GET IN TOUCH

AHT Tech

AHT Tech

Andrew Quach
Director of Consulting



EMAIL ADDRESS

andrew.quach@arrowhitech.com



PHONE NUMBER

+84 934 1777 35



WEBSITE

www.arrowhitech.com

QUESTIONS?