PCI DSS

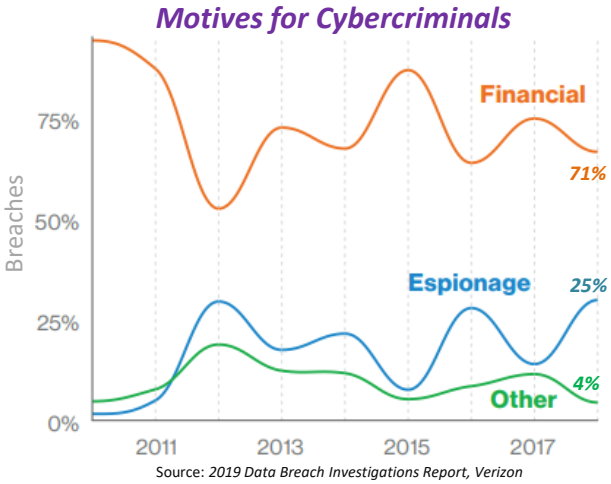
Protecting your customers payment data

WINGO STARR GROUP

PCI DSS Compliance in APAC

*According to **Verizon's 2019 Payment Security Report (2019 PSR)**, organizations compliance in the Asia-Pacific (APAC) region were at 69.6%*

*Merchants that process, store or transmit credit card data is **required** to be **PCI compliant***



Source: *2019 Data Breach Investigations Report, Verizon*

SUMMARY

Payment Card Industry Data Security Standard (PCI DSS) is a global card industry security standard, established by five major international payment card brands, Visa, MasterCard, American Express, JCB International and Discover, to enhance cardmember data and transaction data security.

PCI DSS is a set of requirements created to help protect the security of electronic payment card transactions that include personal identifying information of cardholders and operates as an industry standard for security for organizations utilizing credit card information.

PCI DSS applies to ALL companies that accept, process, store or transmit credit card information.

THREATS

Top motive for a cybercriminals is money: 71**%** of the data compromised during 2018 was financial and payments-related. The rest of the compromised data are espionage (**25%**) and others (**4%**) according to Verizon's Data Investigations Report, 2019.

These data points to retail and hospitality sector being a prime target for hackers as they hold large amount of payment card and customer data.

PCI DSS

Protecting your customers payment data

CASE STUDY
(The need for PCI DSS)

"MARRIOTT FACES A CLASS-ACTION SUIT AND SHARES HAVE SUBSEQUENTLY FALLEN 5.6%. ON TOP OF THIS, MARRIOTT SAYS FOR ABOUT 327 MILLION VICTIMS, COMPROMISED DATA MAY INCLUDE UNENCRYPTED NAMES, ADDRESSES AND PASSPORT NUMBERS WERE INCLUDED IN THE INFORMATION ACCESSED BY AN UNAUTHORIZED THIRD PARTY."

Forbes, December 2018

PCI DSS Compliance Support

Please contact us for advice, if you are:

- *Businesses processing payment card transactions*
- *Concerned with increasing cybersecurity threats and regulations*
- *Requiring assistance*

Our team of experts have decades of experience in building information security programs that work with business objectives and show measurable improvement to security posture

WHAT ARE THE GOALS OF PCI DSS?

Failing to maintain PCI compliance can cause your company to be subject to a class action lawsuit and/or a fine of up to $5,000 to $100,000 a month (that your company is in violation) in addition to the inevitable loss of business that happens when a data breach compromises customer payment information.

There are four (4) levels of PCI DSS compliance based upon how many payment card transactions are processed in a year by the entity:

Level 1 **6 million + Transaction/year**	**Level 2** 1 to 6 million Transaction/year
Level 4 Under 20,000 Transaction/year	**Level 3** 20K to 1 million Transaction/year

WHAT ARE THE GOALS OF PCI DSS?

There are four (6) main goals set for PCI DSS compliance:

- **Build and maintain a secure network and systems**
- **Protect cardholder data**
- **Maintain a vulnerability management program**
- **Implement strong control access measures**
- **Regularly monitor and test networks**
- **Maintain an information security policy**

HOW AND WHERE TO START?

You can start by adopting and implementing a 'best practices' at your organization-

- SCOPE: Determine business requirements
- INVENTORY: Know where your information assets are stored
- REVIEW & UPDATE: Policies and Procedures
- AWARENESS: Educate and Train

WINGO STARR GROUP

Contact: enquiry@wingostarrgroup.com

Wingo Starr Group Sdn Bhd, (1151046-X)
Level 17, Tower B (Plaza Pantai)
Persiaran Pantai Baru, Off Jalan Pantai Baru,
59200, Kuala Lumpur, Malaysia
Website: www.wingostarrgroup.com
Email : enquiry@wingostarrgroup.com