WINGO STARR's Virtual CISO

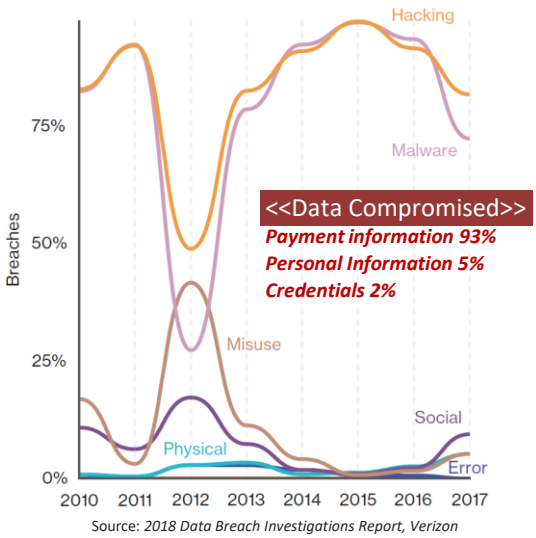
Protecting the hotel and hospitality industry with security controls

WINGO STARR GROUP

CYBERSECURITY IMPACT TO HOSPITALITY SECTOR

According to PwC's Hotels Outlook report, 2018-2022, the hospitality industry has the second-highest number of cybersecurity breaches after the retail sector.

Types of breaches seen in the accommodations sector



Source: *2018 Data Breach Investigations Report, Verizon*

SUMMARY

Hospitality industry are a prime target for cyber criminals due to the fact that they hold a wealth of personal and financial information on its customers while almost all aspects of their daily operations are computerized.

In the accommodations sector, the revenue of the global hotel market was reported at 495.17 billion U.S. dollars in 2016, offering cyber-criminals a lot to gain from a successful data breach. In addition, many hotels are franchised out to independent owners who do not utilize the most secure systems and often outsource IT services to companies that are not equipped to respond to a data breach quickly and efficiently.

INTRODUCTION

While hotels have a strong handle on the physical security of their guests, are they as dedicated to protecting these guests' data?

According to a study by Trustwave in 2016, the hospitality industry accounted for the second highest number of cybersecurity breaches after the retail sector.

Individuals who work in the sector are rarely IT people having limited knowledge of information security.

COMPLEX PROBLEMS

As cyberattacks become more common, there's a growing concern of how to stop them.

Hackers and other cybercriminals are developing increasingly sophisticated methods to breach organizations' computer networks in order to steal data, halt operations, hold data to ransom or all of the above. Unfortunately, while the manufacturing sector has traditionally not been a target, that's no longer the case. With the rise of smart factories, hackers have more and more opportunities to gain access to your network.

The following are trends and threats to look out for in 2019, predicted by industry professionals:

Point-of-Sale Attacks

Attacks on the point of sale (POS) system of a hotel are one of the biggest cybersecurity threats to the hotel industry if not properly secured

Evolving Ransomware

Ransomware has persisted for so long both because it can be used to such devastating effect and for its relative simplicity

Phishing

Phishing is one of the most common online fraud tactics developed over the past decade and will continue in 2019

Biometric Data Theft

As biometric logins become more common, hackers will take advantage of their use as a single-factor method of authentication

IoT (Internet of Things) Attacks

Connected devices are handy for consumers and companies, but once controlled by hackers, they can be overloaded or locked down, causing havoc

Theft of information over Wi-Fi

Hotel Wi-Fi to guests are vulnerable to Hackers attack – they can easily access and take advantage of a weak Wi-Fi connection to gain access to personal information

LAWS, DIRECTIVES AND COMPLIANCE

Malaysia, Laos, the Philippines, Thailand and Vietnam already have in place standalone cybersecurity legislation. Cambodia has a draft cybercrime law that has not come into effect yet, and Myanmar and Indonesia have each adopted laws on electronic transactions that contain provisions on cybercrime.

ASEAN is diverse, and Asia even more so. Given the varying stages of development in cybersecurity policy and laws across the region, businesses will need to track closely any laws that may be introduced or amended within each jurisdiction in which they operate.

Businesses should consider conducting cybersecurity tabletop exercises with key personnel across relevant departments to ensure that these stakeholders are well prepared and know how to respond in the event of a data incident, with a view to minimizing any resultant losses that may be suffered by the business.

External professionals should also be retained to give advice on any legal implications, for instance, regarding the provision of information to the regulator during the course of an investigation, preserving confidentiality over commercially sensitive information or claiming privilege over relevant documents.

Cybersecurity Laws in Asia


The Cybersecurity Act, B.E. 2562 (2019)


Cybercrime Prevention Act 2012


Regulation Number 82 of 2012
Provision of System and Electronic Transactions


Cybercrime Law (drafted 2018)


The Cyber Security Law 2019


New cyber law under consideration


Computer Crimes Act 1997

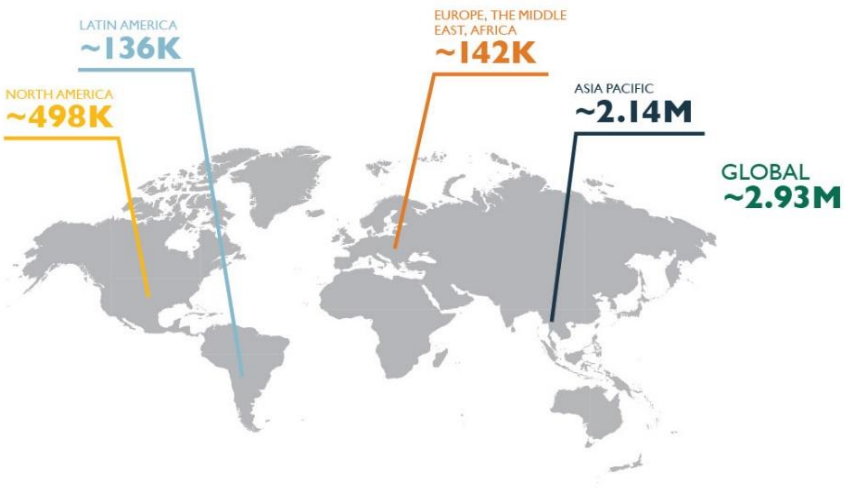

Cyber Crime Law 2015

SHORTAGE OF SKILLED PROFESSIONALS

There is a growing problem is the shortage of cybersecurity workers, putting people and companies at risk.

Some companies are using the skills and professional shortage as an excuse to enable lax security strategies, causing an even greater risk for their company.

(ISC)^2, the world's largest association of cybersecurity professionals, predicts the cybersecurity workforce gap has increased to more than 2.9 million globally, while the Asia-Pacific region is experiencing the highest shortage at 2.14 million.



Source: (ISC)²'s Cybersecurity Workforce Study, 2018

SKILL SHORTAGES, A SECURITY RISK

The cyber crime epidemic has escalated rapidly in recent years, while companies and governments have struggled to hire enough qualified professionals to safeguard against the growing threat. This trend is expected to continue through 2019 and beyond

Protecting the hotel and hospitality industry with security controls

CASE STUDY

"Marriott Provides Update on Starwood Database Security Incident - Marriott now believes that approximately 5.25 million unencrypted passport numbers were included in the information accessed by an unauthorized third party."

Marriott International News Center Jan 4, 2019

Virtual CISO – 'vCISO'

Businesses concerned with increasing cybersecurity risks and regulations, but having budget restrictions may want to turn 'vCISO' for strategic guidance

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

SECURING CORPORATE DATA

Managing cybersecurity in today's world is almost indescribably difficult. What was once only the computer and maybe even storage media, has now ballooned into the internet.

As all these becomes a part of how we work and interact, the points that information can be compromised increases.

While there are IT employees who may have a hold on security tool implementations, these roles are a technical "generalist". What you really need is a security specialist, a Corporate Information Security Officer (CISO), capable of prioritizing both the business and the security of information, infrastructure, sensitive data and your public reputation, and minimizing the risks to all of these before a breach occurs.

MINIMIZE EXPOSURE TO SECURITY THREATS WITH VIRTUAL CISO

With Cyber security continuing to affect organizations from large enterprises to small and medium business's (SMB) the role of a CISO is becoming more important than ever.

In order to protect the corporate data and comply with regulatory requirements, companies should employ a dedicated CISO, but for many SMBs and budget conscious companies, a full time CISO is beyond their budget.

A virtual CISO – 'vCISO' may be the solution for you

vCISO is an outsourced information and cyber security practitioner/provider who offers their knowledge and insight to an organization on an on-going or on-demand basis.

The service is designed to make top-tier security experts available to organizations who need security expertise and guidance. The following are some of key measures to keep your information secure and protected from cyber threats:

- Starting a cybersecurity risk assessment based on your organization's assets
- Building a cybersecurity plan and program
- Building a Governance, Risk and Compliance (GRC) program
- Focusing on people including managing personnel, contractors and/or vendors
- Building and executing a training strategy

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