

# *PERSIDANGAN JURUAUDIT SEKTOR AWAM TAHUN 2017*

Sesi IV: Cabaran  
Pengauditan Terkini (2017):  
Cyber Threat and Technology

---

# *Agenda*

- Definition of Cyber Threat
- Background
- PwC's View
- Conclusion

---

# *Definition of Cyber Threat*

## Cyber threats



Information  
Technology (IT)



Operational  
Technology  
(OT)

- *Cyber threats are not new but the attack methods have become more sophisticated and widespread overtime as adoption of technology continue to surge.*
- *Cyber threats do not only affect the corporate Information Technology (IT) systems. For industry such as energy, mining and utilities, there are just as significant security threats to operational technology. The term ‘operational technology’ (OT) refers to the hardware and software used to control industrial processes.*

---

# *Background*

# Cybersecurity

## What concerns the senior business and technology executives today?

In our 2018 Global State of Information Security® Survey (GSISS), leaders of organizations that use automation or robotics indicate their awareness of the potentially significant fallout of cyberattacks.

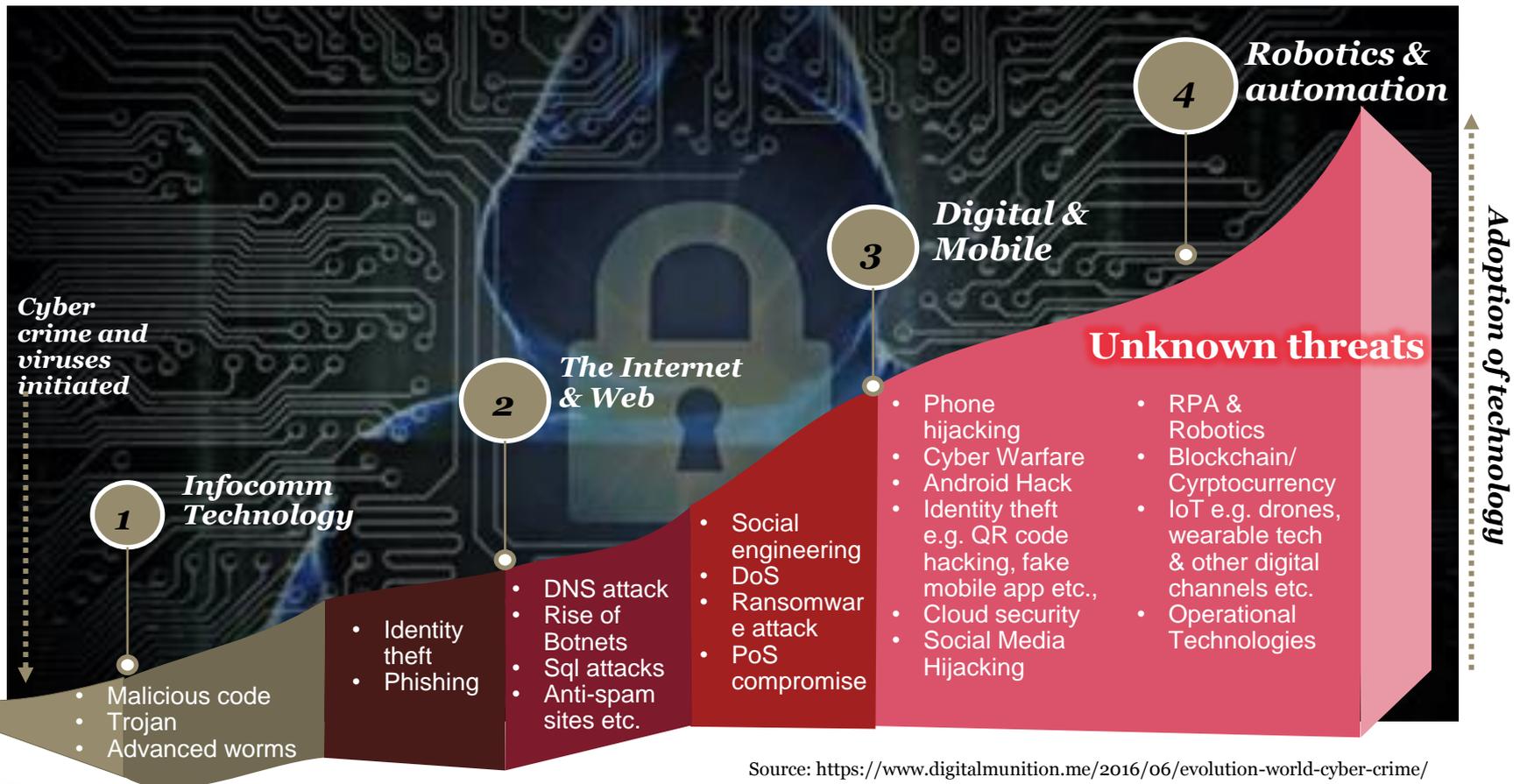
### Anticipated results of a successful cyberattack against automation and/or robotics systems



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 18, 2017.  
Base: 9,500 respondents

# Cybersecurity – Past, present and future

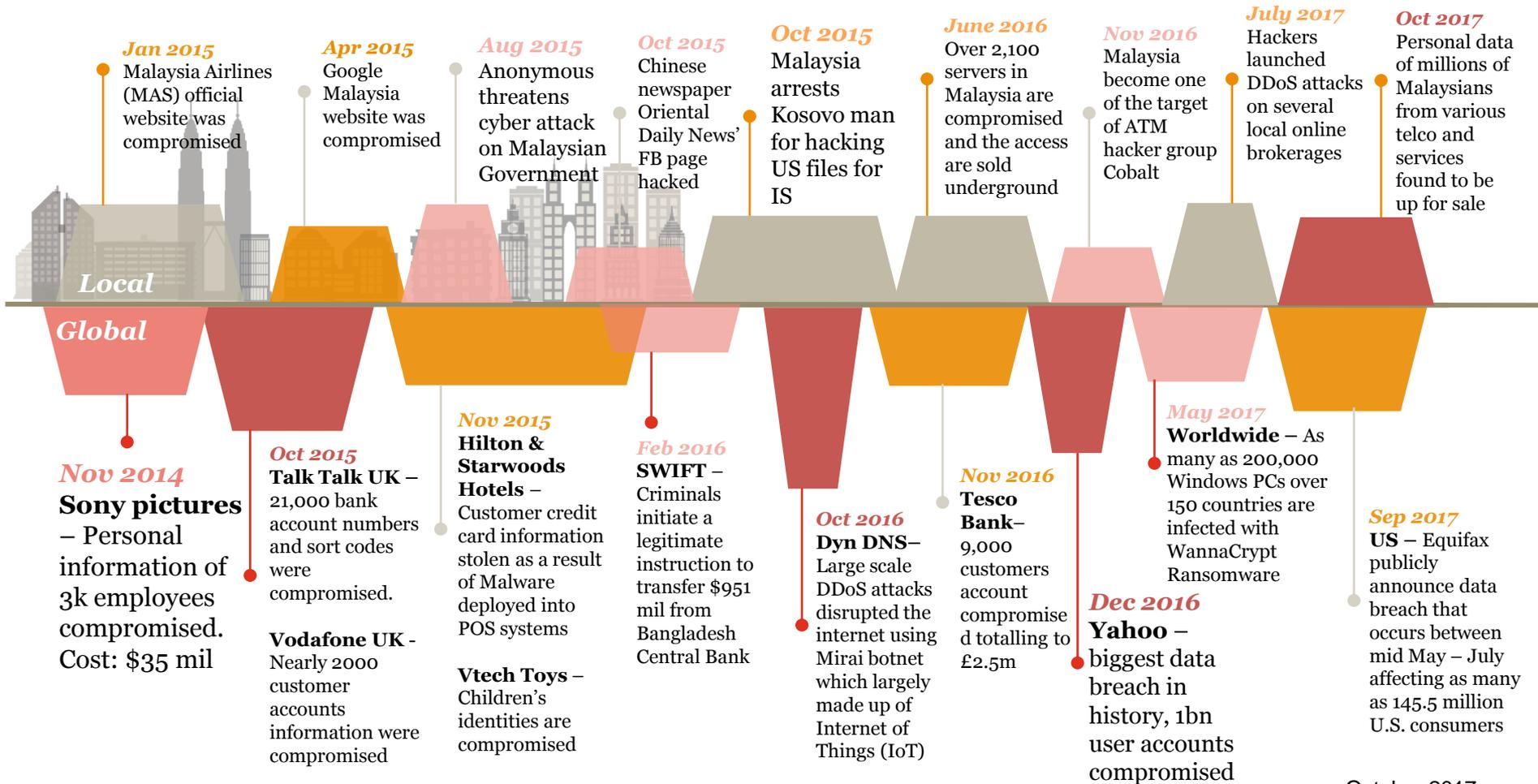
Top vector of cyber threats faced by organisation over the years?



Source: <https://www.digitalmunition.me/2016/06/evolution-world-cyber-crime/>

# Cybersecurity attacks that made headlines..

Cyber attacks are getting headline coverage globally & locally



# *Cybersecurity attacks that made headlines..*

Operational security issues leading to business disruption

## *Power & Utilities*

**August 2017**

The Irish power grid was attacked.

**July 2017**

Digital assault on U.S. energy companies, including a nuclear power plant.

**December 2015**

First known successful cyberattack on a power grid in. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers.

## *Telecommunications*

**May 2017**

Telefonica of Spain had been infected with malicious software i.e. “ransomware” which locks up computers and demands ransoms. The ransomware attack also hit telecom companies in Portugal, Megafon in Russia

**Since 2014**

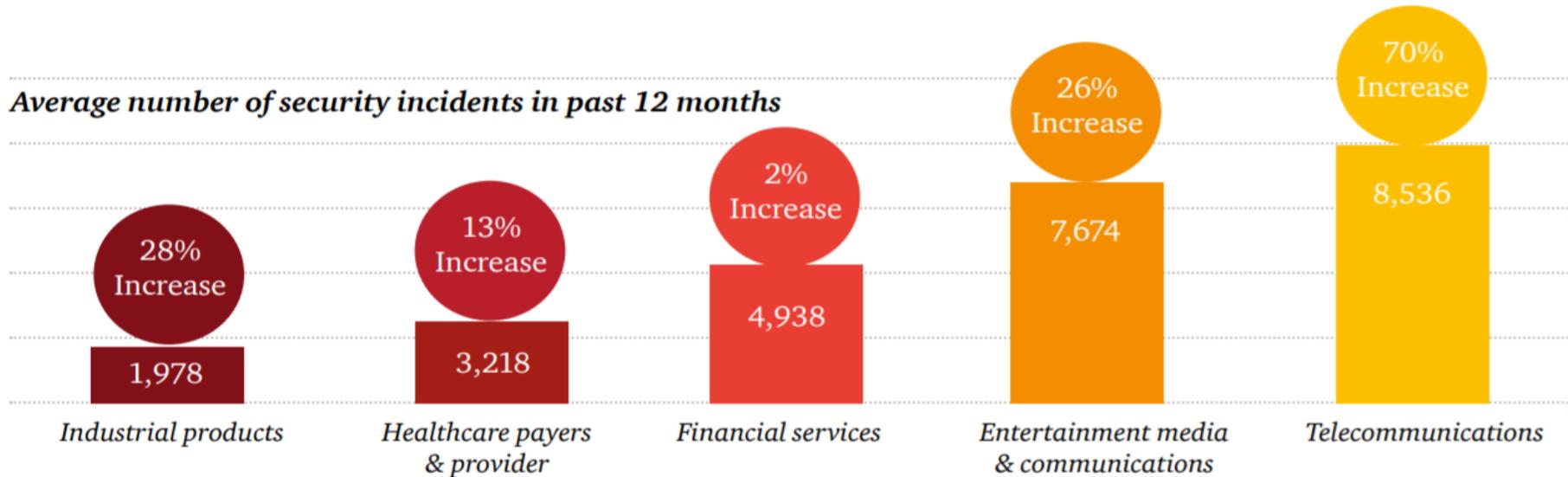
In 2017, telco infrastructure security flaw “SS7” was exploited by hackers to drain O2-Telefonica customers' bank accounts, intercepting the multi-factor authentication

---

# *PwC's View*

# *PwC Global State of Information Security Survey 2017*

## Average number of security incidents in past 12 months



*\*A security incident is defined as any adverse incident that threatens some aspect of computer security.*

*The Global State of Information Security® Survey (GSISS) 2017 is a worldwide study by PwC, CIO and CSO. It was conducted online from April 2016 to June 2016. Readers of CIO and CSO and clients of PwC from around the globe were invited via email to participate in the survey. Amongst the 10,000+ respondents participated in the survey, ~60 were from Malaysia.*

# *Cybersecurity*

## What auditors should be doing?



*“Accountants have a number of skills that are relevant in cybersecurity. Among other skill-sets and areas of expertise, accountants are excellent at inventory, which translates into helping business and IT team to ensure all systems are properly updated and protected. Accountants’ skills in audit can also help boost a company cybersecurity’s ongoing monitoring.”*

*- Lisa Traina, Partner at Traina & Associates (Extracted from IFAC Global Knowledge Gateway)*

# ***Cybersecurity***

What auditors should be doing?



**Public Company Accounting Oversight Board (PCAOB)**

*“There are no required audit procedures related to cybersecurity.”*

However, auditing standards require us to obtain or update our understanding of the entity and its environment, and to understand the events, conditions, and activities that might reasonably be expected to have a significant effect on the risks of material misstatement – including cyber related events.

# *Cybersecurity*

## What auditors should be doing?



### **AICPA Unveils Cybersecurity Risk Management Reporting Framework**

Voluntary Engagement Will Help Companies and Auditors Communicate Cyber Risk Readiness

*Published April 26, 2017*

**NEW YORK (April 26, 2017)** – At a time when organizations around the world are facing cybersecurity attacks, it is more important than ever for them to demonstrate to key stakeholders the extent and effectiveness of their cybersecurity risk management efforts. To help businesses meet this growing challenge, the [American Institute of CPAs \(AICPA\)](#) has introduced a market-driven, flexible and voluntary cybersecurity risk management reporting framework.

“Cybersecurity threats are escalating, thereby unnerving boards of directors, managers, investors and customers of businesses of all sizes – whether public or private,” said [Susan S. Coffey, CPA, CGMA](#), AICPA executive vice president for public practice. “While there are many methods, controls and frameworks for developing cybersecurity risk management programs, until now there hasn’t been a common language for companies to communicate about, and report on, these efforts.”

# *Changing the cybersecurity focus from technology to business/operational risk*

Leading firms are seeing significant benefits in shifting their focus from Cyber Security being seen as a IT problem, managed separately by technology operations, to a more business/operational risk focus, enabling them to be more pro-active and effective in managing cyber risks.

*Typical effective maturity evolution*



**Current**

**Target**

## *Technology Operations Focused*

- Part of IT Operations
- Handles technical and tactical aspects of Security
- Focus is on fire-fighting
- Goals: Lower costs, achieving operational efficiency

## *Information Risk Focused*

- CISO report into the CIO with a dotted-line relationship to enterprise risk management
- Focus is on defining, maintaining and monitoring policies
- Goals: Regulatory compliance, building security into architecture

## *Business / Operational Risk Focused*

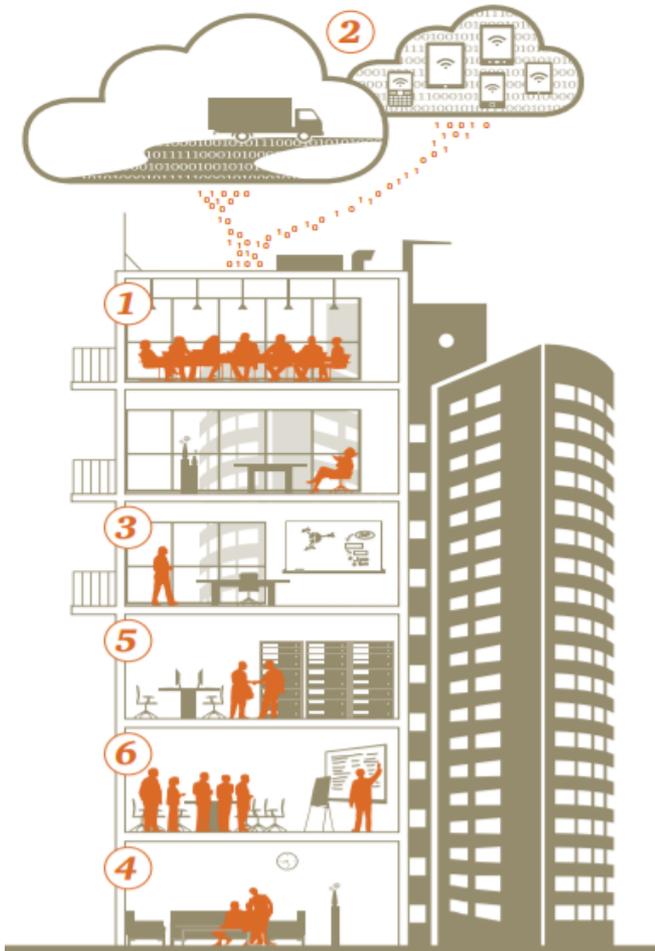
- Aligned with Operational Risk
- Aligned with Information Governance
- CISO maintains authority and visibility; peer to CIO
- Focus is on understanding business needs
- Goals: Proactive risk management and anticipating business needs
- Information security is a business priority

---

# *Conclusion*

# Cybersecurity

## Our recommendations



1. **Tone at the top** – solid cyber risk governance and view cyber risk as a business issue
2. **You can't protect what you don't know** - know your critical assets and cyber organisation boundaries
3. **Gather intelligence** - Stay ahead of cyber threats
4. **Security as a routine** – collect, analyse, report, prevent/improve
5. **Plan & respond** – Develop playbook, play-out threat scenarios, cyber-insurance

---

# *Thank you*

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Risk Services Sdn Bhd, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2017 PricewaterhouseCoopers Risk Services Sdn Bhd. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Risk Services Sdn Bhd which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.