CYBER SECURITY

FACILITATING YOU IN SECURING CLP'S BUSINESS

Recipe for a Successful Cyber-Safe Awareness Campaign

25 November 2016

燃點生活力量
Energy for Life

CLP 中 中電

Disclaimer

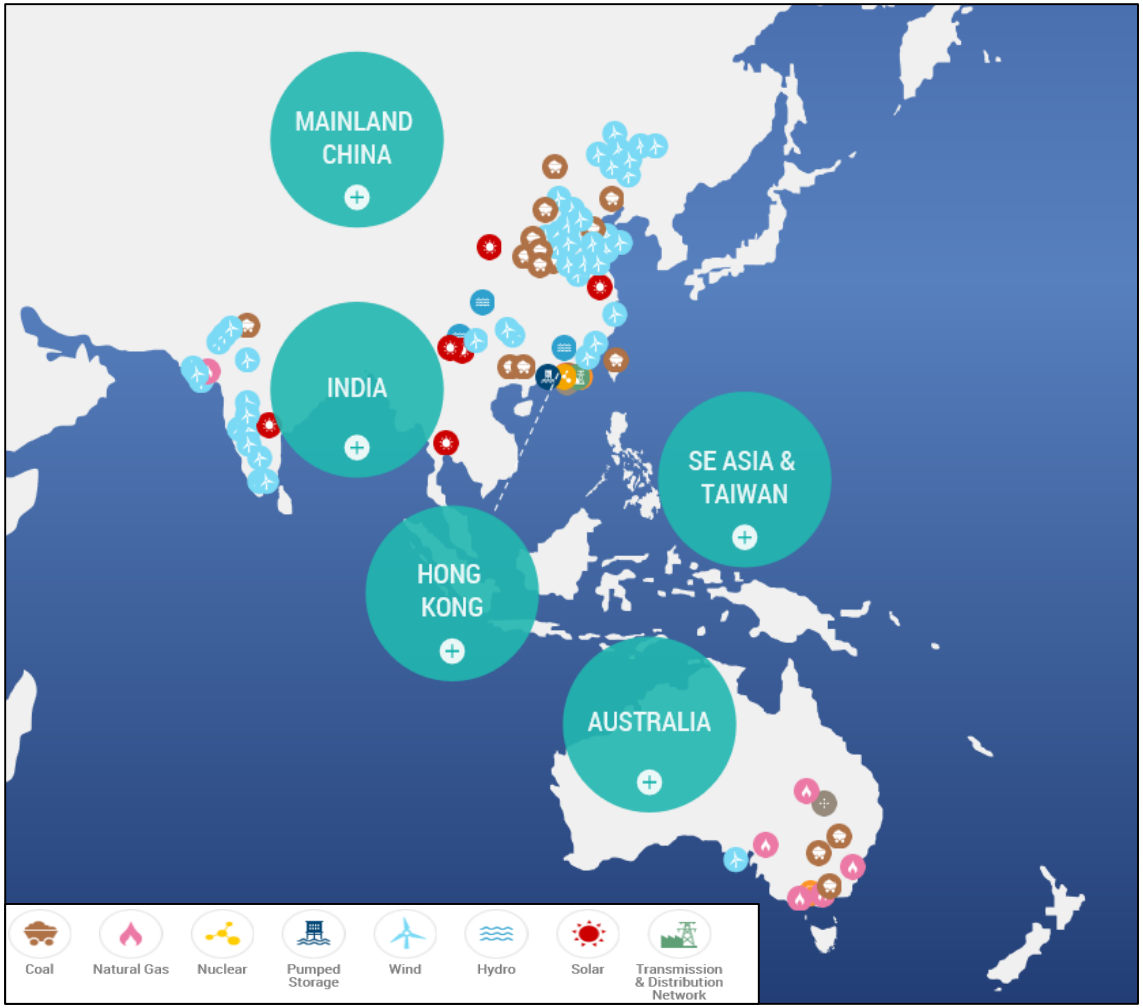
This presentation including all images serves as information sharing only.

In case there are individuals, organisation names and/or technology brand names mentioned during the talk, this does not represent CLP's endorsement, recommendation or criticism of these entities….

Any control mechanisms, processes or technologies mentioned should not suggest that CLP is more or less secure than our industry peers or global competitors.

About CLP – Assets at a glance

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS



Source: www.clpgroup.com

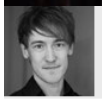
燃點生活力量
Energy for Life

CLP 中電

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

7 JUN 2016 NEWS

#infosec16: Security Awareness Raising a Waste of Time, Say Experts



Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

Security awareness and training programs are mostly ineffective and a waste of time and money, according to a panel of experts speaking at Infosecurity Europe in London today.

Experts agreed that the way to address these problems is to make programs more relevant to their audience in a way which will help to build an organization-wide culture that makes security second nature to employees.

Angela Sasse, director of the UK Research Institute in Science of Cyber Security (RISCS) at UCL, argued that it was "very doubtful" that most programs had any value at all and said government-led efforts aimed at educating the populace were "pitiful" and sent out mixed messages.

The focus should be on changing people's behavior rather than raising awareness, as the latter does little to improve information security, according to Andrew Rose, CISO in the UK transport sector.

He said program managers could take a leaf out of the marketer's book in looking at new ways to influence behavior in smaller, bite-sized chunks – in an almost subliminal way that doesn't require hour-long training sessions.

Rose said his team inform all infosecurity training via a simple three-point framework: "motivation," ie what are the consequences of a specific policy; "ability," ie can employees practically comply with any new rules; and "triggers" – what will remind them to do the right thing?

Uber's security awareness and education program manager, Samantha Davison, argued that training has to be as relevant as possible to employees so as to avoid wasting everyone's time by resulting in programs that don't work.

The taxi hailing firm builds its programs on the back of feedback from staff, and is currently developing a training app which will produce different content depending on the location and role of the individual user, she explained.

"Build a program they want, not the program you want as an information security professional," she advised.

Publicis Groupe CISO, Thom Langford, added that building a corporate culture around security best practice is the goal.

"Culture is great; it's also really difficult to build, but once it's built it lasts a long time," he argued.

This will ensure security is maintained almost subconsciously by staff, and one of the ways to get there is by creating "visceral experiences" through new approaches to training, he said.

UCL's Sasse concluded that although improvements to training programs are a necessity – not least because the "attackers are getting more persistent and smarter" – they won't be a cheaper option.

To be most effective, training programs must be built on the back of the right corporate technology "which wastes people's time as little as possible," she argued.

Is it a familiar comment to you?

燃點生活力量
Energy for Life

CLP 中電

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

Don't make an awareness programme

Make a BEHAVIOUR/ CULTURE CHANGE PROGRAMME

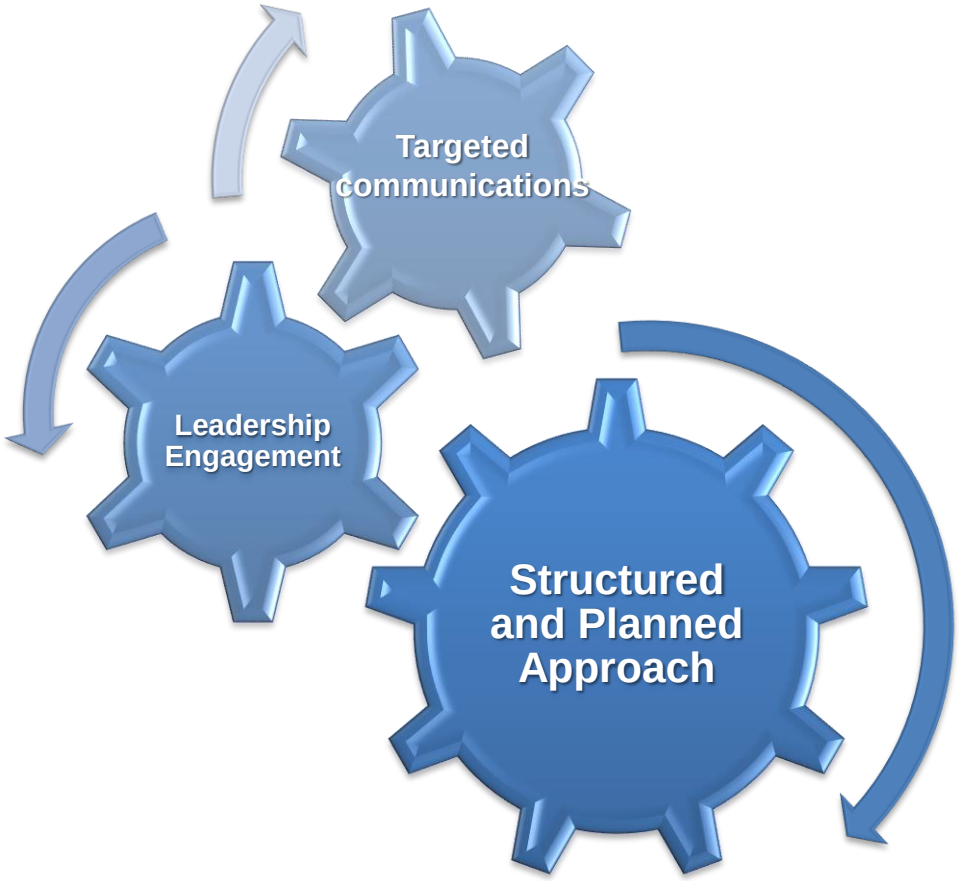
燃點生活力量
Energy for Life

CLP 中電

Ingredients:
Proven Change Methodology

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

- ✓ Proactive identification of training needs
- ✓ Proactive identification and management of employee resistance



燃點生活力量
Energy for Life

CLP 中 中電

Ingredients:
Change Curve

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

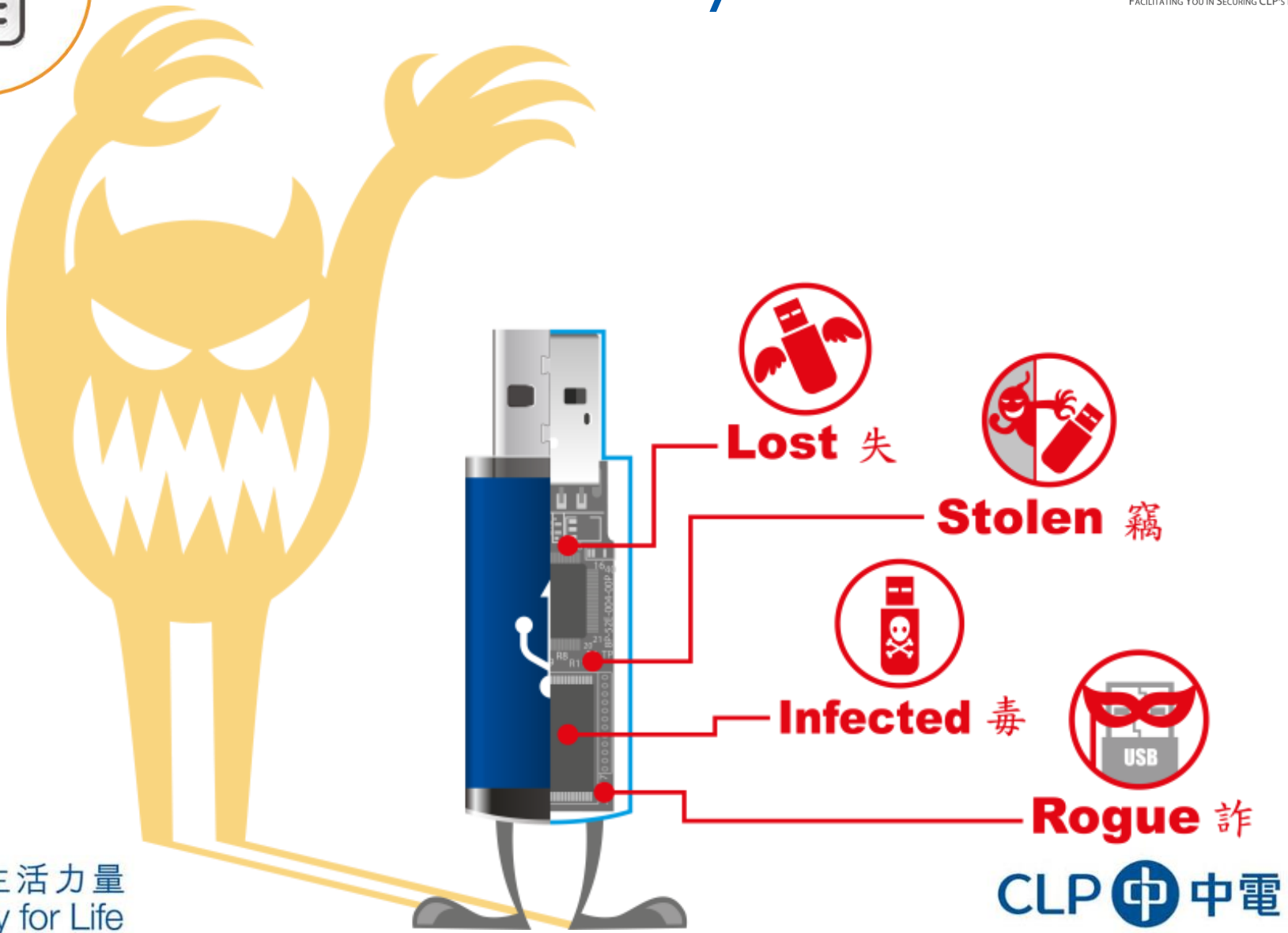
Source: PROSCI ADKAR model

燃點生活力量
Energy for Life

CLP 中 中電

Ingredients: Creativity

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

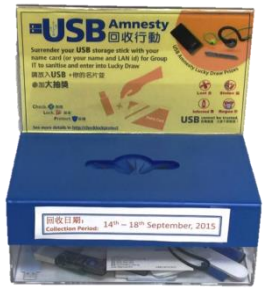


燃點生活力量
Energy for Life

CLP 中 中電

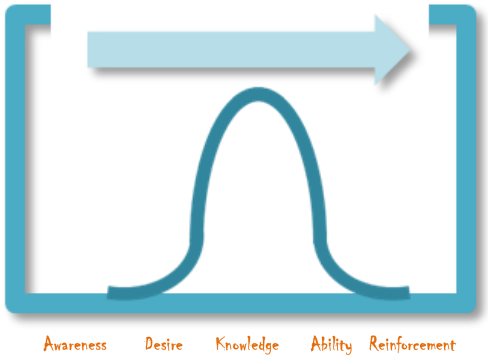
Ingredients:
Key Success Factors

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS



No. of USBs Collected

No. of Video View Counts



Change Curve Distribution

Need to be measureable, enabling trend comparison. Consider a post implementation survey every year!

燃點生活力量
Energy for Life

CLP 中 中電

Directions : Identify your risks

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

2010 Aug: Iran nuclear plant centrifuge destroyed by Stuxnet via USB infection. Detail here

2012 Feb: U.K. nuclear plant lost data in USB. Detail here

2012 Oct: Crimeware in USB idled U.S. power plant for 3 weeks: link

2013 Nov: International Space Station infected by USB malware: link

2010 2011 2012 2013 2014 2015 2016

2014 Aug: New USB Threat - 'BadUSB' found: Detail here Explanation Video

2014 Nov: New USB Threat - Cyber Espionage use 'USBStealer' to steal data from Closed Networks. Detail here

2015 Nov : New USB Threat - 'USB Killer' destroys computer in seconds: Detail here

2016 Mar: New USB Threat - 'USB Thief' data stealing malware: Detail here

2016 Apr: German Gundremmingen Nuclear Plant with USB infection. Detail here

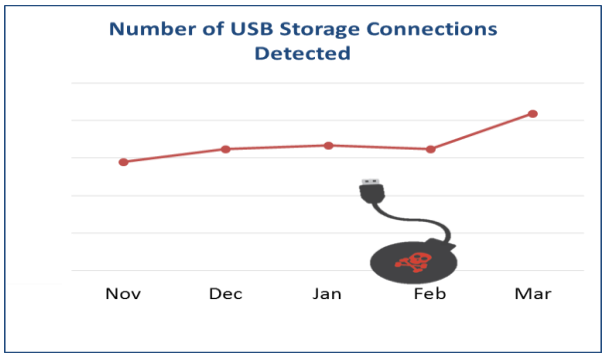
... Keep on sharing industry real-life incidents

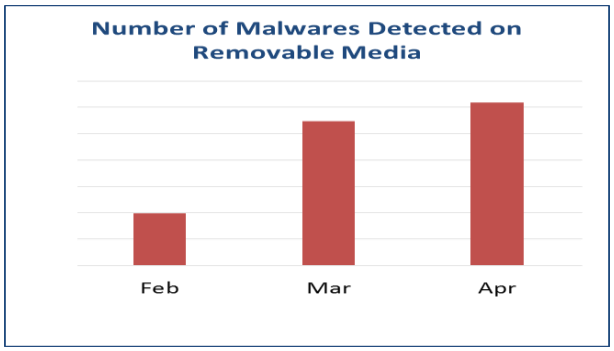
燃點生活力量
Energy for Life

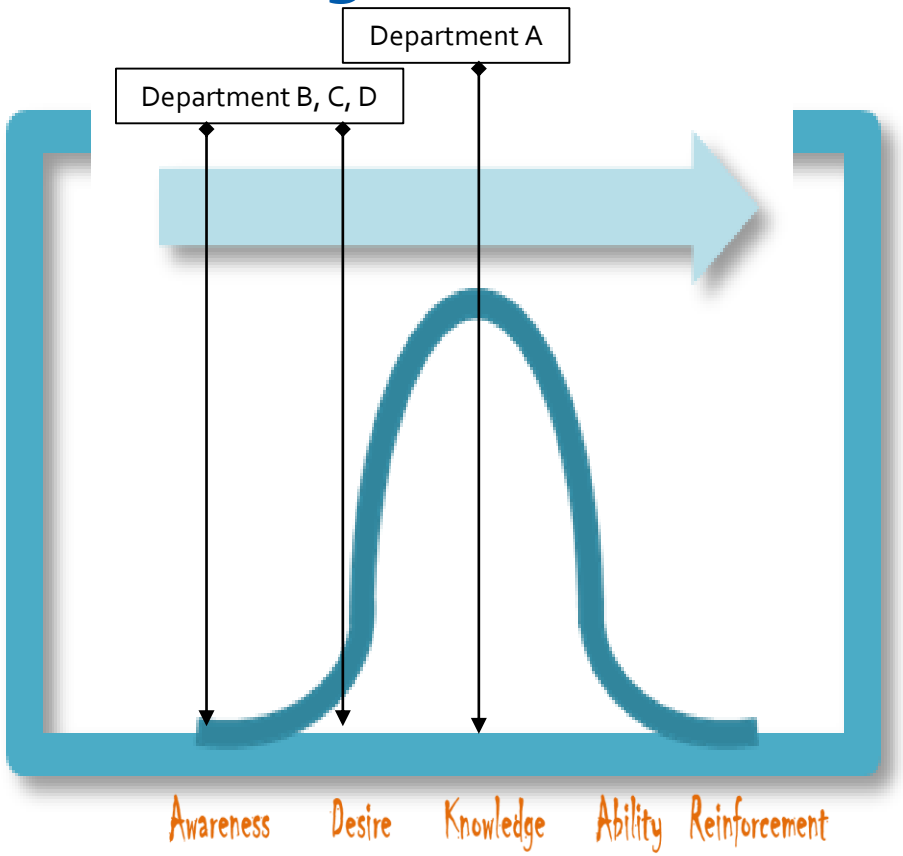
CLP 中 中電

Directions :
Map stakeholders on change curve

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS







Mapping per current behaviour, for example infected or unattended USBs found by department

燃點生活力量
Energy for Life

CLP 中 中電

Directions :
Set target key messages

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

Everyone can help to take one more step the company

Sub-messages

1. USB malware is now a very common attack, which can cause serious damage. [Aware & Desire]
2. Wide adoption of USB in company presents huge risks. [Aware & Desire]
3. Together, we need to stop using USB storage to protect the company. [Aware & Desire]
4. We can minimize impact to operation by Smart Alternative. [Knowledge]
5. We will continue to monitor the risk to strengthen our security [Reinforce]

Communication Calendar

		Year											
	Sub-Activities	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
All Staff	Video												
	Poster												
	Email						●						
	Broadcast				●	●				●			
	Meetings				●	●			●				
	Team Briefing (Monthly)						●	●		●			
	Survey											●	
Management	Focus Group Meeting		●				●				●		
	Executive Newsletter					●						●	
	Executive Update					●				●			
Technical users	Champion Meetings						●						
	PCC Meetings			●				●				●	

Make your key message, sub-messages, activities which would drive the messages across. Form the final communication plan & calendar.

燃點生活力量
Energy for Life

CLP 中電

Make it personal

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

Threat

Cyber Security is our shared responsibility

In ancient times, when a castle was stormed, every person was armed to fight and protect – even the king.

燃點生活力量
Energy for Life

CLP 中 中電

Make it to their personal life also

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS


CLP 中電

CYBER SECURITY

CST EXPRESS 網絡安全快訊

FACILITATING YOU IN SECURING CLP'S BUSINESS 助你維護網絡安全，確保中電業務運作 QUARTER 1 第一季 2015

The Cyber Security Team prepares this quarterly CST Express newsletter for all staff in CLP Group, including Hong Kong, Australia, China, India and South East Asia.

網絡安全小組為中電集團 — 包括香港、澳洲、中國、印度及東南亞全體員工，準備了此期網絡安全快訊季度報訊。

Can we really trust a USB ?
我們真的可以信任USB記憶棒嗎？

The ease of use and widespread adoption of USB sticks has created a false comfort that these devices are safe. While anti-virus software available on computers may protect against an infected USB, there is no protection from sensitive data loss when a USB is forgotten or lost.
USB記憶棒廣泛使用，使用簡便，但在令人誤以為這些裝置很安全。雖然電腦上的防毒軟件有機會抵禦USB感染惡意的病毒，但如果USB被遺忘或丟失，則當中的敏感資料也一樣會遺失。

Furthermore, hackers are so sophisticated nowadays, USBs are also used as
另外，當今駭客的手段非常高超，還得利用USB記憶棒作以下用途：

A simple method of virus spreading
作為散播病毒的簡單方法
(refer to Page 2 for more on how the Stuxnet infection caused a overspinning of centrifuge in a Iran nuclear plant)
(參閱第2頁，了解Stuxnet病毒如何導致伊朗一個核電站的離心機機械過快而損毀)

A camouflage as an external keyboard or network adaptor in order to carry out malicious hidden actions
偽裝成外部鍵盤或網絡介面卡，以進行惡意的隱蔽行動
(refer to Page 4 for the latest risks found on USB)
(參閱第4頁，了解在USB上發現的最新風險)

Use of USB becomes the biggest ever cyber risk
USB構成歷來最大的網絡風險

Source 資料來源：BBC News

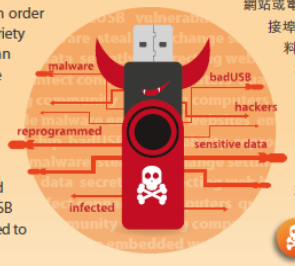
The computer hacking community has been able to demonstrate a simple method for infecting computers via USB, proving that these trusted devices were no less vulnerable than malware embedded websites or emails. Most users know that their USB port accepts a wide-range of peripheral devices, i.e. printers, data storage thumb sticks, webcams, keyboards, cell phones etc. In order for the computer to interact with the variety of devices, USB ports will negotiate an agreement or handshake which must take place between the USB controller chip on the USB device and the computer.

The fact is that a so-called "badUSB" vulnerability – allowing these controller chips on USB devices to be reprogrammed – has now been found. It means that a USB thumb drive's controller chip can be altered to make the computer believe that:

- The stick is a keyboard, issue its own commands, including instructions to install malware or steal files
- The stick is a network card, change a computer's setting and secretly sending your sensitive data out by redirecting your web browsing traffic

It can even infect connected computers at bootup, before any antivirus tools can detect it and "quarantine" it.

The USB manufacturers are considering to produce new products with signed firmware, thus to differentiate trusted devices from untrusted one. However, simply by external appearance, how can a general person or consumer can tell this difference?



黑客能簡單地利用USB裝置，使電腦感染病毒。這點證明USB這種頗受信任的裝置，其危險性並不遜於已嵌入惡意程式的網站或電子郵件。大多數使用者知道，他們的USB連接埠接受各式各樣的周邊裝置，例如列印機、資料儲存記憶棒、網絡攝影機、鍵盤、智能手機等。為了能讓電腦與多種裝置互動，USB連接埠會將訊號交換，使USB裝置上的USB控制器芯片能與電腦進行溝通。

事實上，市面上已發現所謂「badUSB」危機，可讓黑客重新編程USB裝置上的控制器芯片。由此，可以令電腦誤以為：

- USB裝置是個鍵盤，發出按鍵指令，包括安裝惡意程式或盜取文檔的指令
- USB裝置是張網絡卡，更改電腦設定，使你在網絡上瀏覽的信息流方向改變，把你的敏感資料秘密發送出去

它甚至可以在電腦啟動之時，當防毒工具還未來得及檢測和「隔離」之前，便感染連接的電腦。

USB製造商正在考慮採用專用韌體來製造新產品，從而區分值得信任與不值得信任的裝置。但單從外表來看，我們或消費者如何能分辨出差別呢？

We all do NOT have **a laser-eye** to examine your USB before using it!

Appreciate your tips to make their personal and families secure

燃點生活力量
Energy for Life

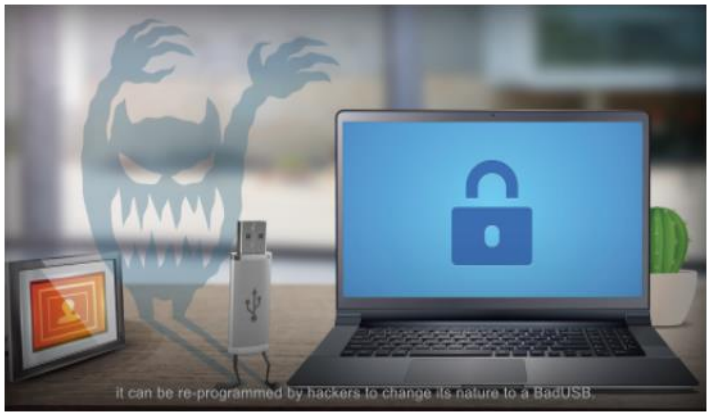
CLP 中電

Directions :

Design activities and communications to move people up the change curve

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

Aware & Desire : Risk of USB



Ability: USB Amnesty / test after training/ tool adoption

Reinforcement: Being Visible

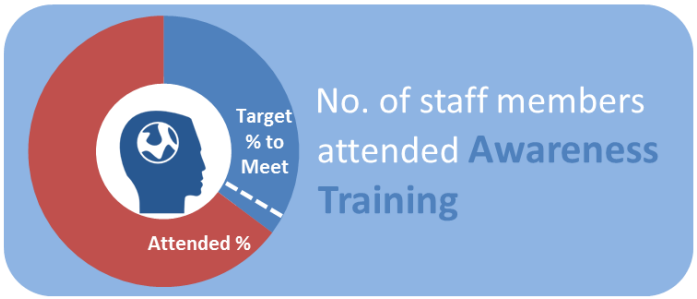
Knowledge: Implement Secure Tools and offer training (Smart Alternative)

燃點生活力量
Energy for Life

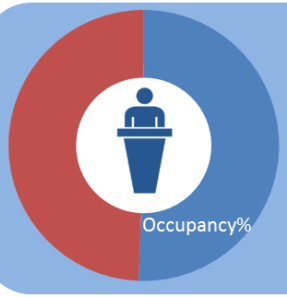
CLP 中電

Directions :
Measure your results

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

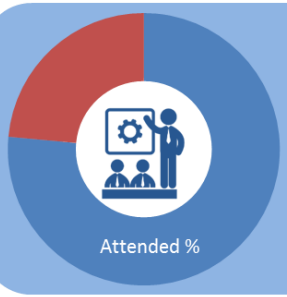


No. of staff members attended **Awareness Training**



No. of staff members attended **Guest Talk**

No. of staff members participated in and completed the **Cyber Security Quiz**



No. of staff members attended **Staff Briefings**

Tool adoption trends, event attendance and survey feedback are valuable to measure if change has happened

燃點生活力量
Energy for Life

CLP 中 中電

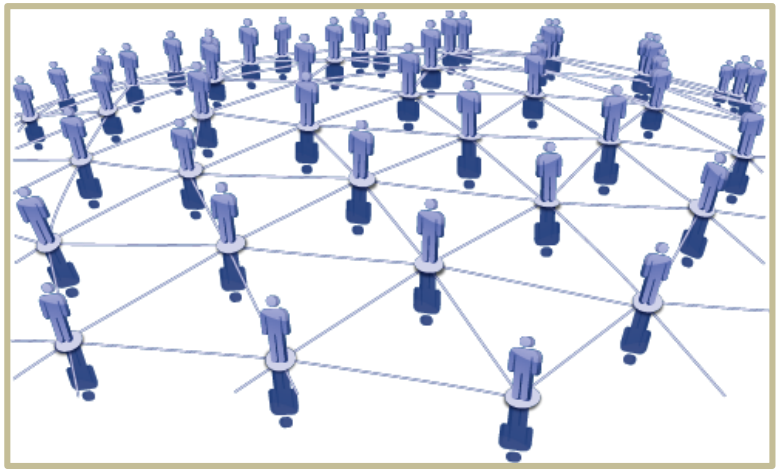
Successful Security Cultural Change

CYBER SECURITY
FACILITATING YOU IN SECURING CLP'S BUSINESS

Ingredients

regularly | all staff | 10 mins/month

- 1 proven change methodology
- 5 stages in change curve
- A lot of creativity
- At least one risk area
- Many key success factors



Directions

- Identify a key risk where a behavioral change would help to mitigate the risk significantly.
- Map your stakeholders on change curve.
- Plan your target messages to different level of stakeholders, make it personal and relevant to them!
- Design activities and communications with a lot of creativity (video, games, posters, newsletters, etc). Make sure they are appropriate for moving people up the change curve.
- Measure your results and change curve position, use them to contribute next round activities.

燃點生活力量
Energy for Life

CLP 中 中電

CYBER SECURITY

FACILITATING YOU IN SECURING CLP'S BUSINESS

Thank you

燃點生活力量
Energy for Life

CLP 中 中電