IS 2184 Information System Management
180329021
Huang, Pei-Yu

Challenges for Organisation in deploying ICTs

Abstract

The role of ICTs deeply affected today's business. However, not every organisation manager acknowledges the risks ICT system may bring when they fail to manage it. ICTs risks from natural disaster to inappropriate use of IT resources, all are serious acts that may compromise the organisation. ICTs security is another imperative factor to consider, the vulnerabilities in the system may lead to the hacking of organisation system and consequently losses confidential data. Managers should have great knowledge in the management of ICTs, understand the know-how of deploying change management when needed, and deliver the knowledge to their employees.

Key words: Information and communications technology, organisation ICTs risks, data security, change management

1. Introduction and Context

ICTs play an imperative role in organisation's everyday business, it enables organisation to collect, process, communicate and consolidate for various purpose. ICT system is an evolutionary and helpful tool for executing organisational plan. For instance, in order to streamline the process of interaction with current and former customers, CRM system is deployed to improve customer services by automated the process, such as automated welcome message, and based on various triggers, the system generates information about the sales or Q&A service. It's also useful for re-engaging with existing customers from the past by sending notification about the latest products and sales to improve the retention rate.

An overall illustration of the roles of organisation ICTs is shown below. (Figure 1.). ICT systems are important for decision making and conduct activities to improve services and gain competitive positioning in markets, however, there are several IT risks that managers will face in deploying ICTs. The paper will discuss the IT risks faced by managers with real life examples and how it should be approached by using change management.

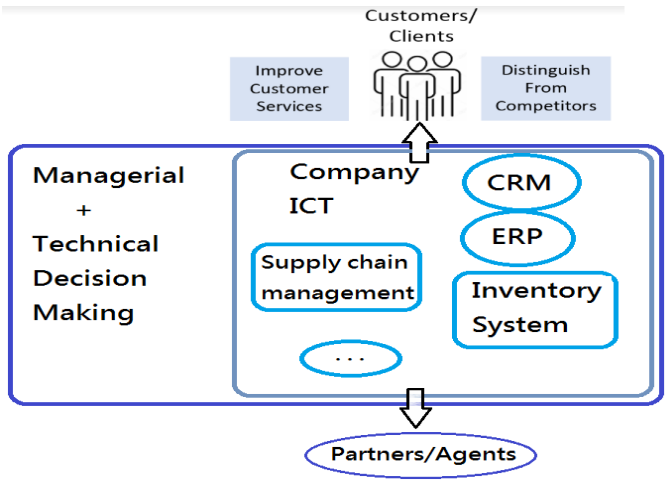

Figure 1. Role of organisation ICT

2. Information systems management issue

Organisations use ICT system to benefit from improvements such as increase working quality, and efficiency in business. However, there are a number of risks should be considered when deploying ICT system.

1) **Incapacity to continue operations due to a natural disaster or accident / Loss of physical assets**
   Natural disasters like earthquake and fire, and accident such as break-in will all causes damage to physical assets or facilities and needs recovery.

2) **Compromise of confidential data regarding organisational plans, products, or services**
   Office devices like IP cameras with vulnerabilities may cause security violation, once the devices are cracked down, it's like paving a way to the whole system and exposing the strategy plans and confidential product details to the criminals.
3) **Incapacity to continue operations due to a deliberated attack**
   Hackers carry out denial-of-service (DDoS) attack to the organisation, which refers to the overwhelming flood of requests, packets or messages send by the botnets to totally saturate the channel and network, thereby denying service to legitimate users such as employees or customers
4) **Compromise of private data of employees or customers**
   Phishing is a common technique for fraud, conducted by malicious email, telephone or text message to lure the victim to provide sensitive data like customer data, login credentials, or download ransom viruses to the victim's computer once click it.
5) **Inappropriate use of IT resources that places firm in a compromising position**
   Employees with lack of knowledge toward organisation's ICTs may cause potential risk. Setting weak password and accidentally downloading malware are all possible ways to place organisation in a dangerous position. Also, employees that use corporate email to disseminate explicit content will cause the organisation subject to lawsuit.
6) **Inappropriate use of IT resources that decrease employee's productivity**
   Wrong decision of deploying ICTs and slack employees, which browse unrelated content at work, is like a chronic disease to the working environment. It takes long-term to discover and make changes, so it will gradually reduce the whole work team's productivity.

The challenges above managers will face are enormous and are hard to predict in the constant changing business environment. As a result, organisations are unable to enjoy the value offered by these ICTs if failed to appropriate deployed. Based upon my study and available sources, point 2), 3) and 4) will be given in next section.

3. Discussion and argument

On TV shows or films, hackers have been portraited as people with grudges who target specific institutions and manually try to break into the system. But in reality, "most of these attacks employ automated scripts that indiscriminately seek out thousands of computers at a time, looking for vulnerabilities." (Cukier, 2007). Vulnerabilities like weak passwords, it makes hackers' jobs much easier, the non-secure usernames and passwords manager use, or employees use gives attackers more chance of success.

3.1 Compromise of confidential data of organisational plans, employees, customers data

Based on my research, many technical reports shown that weak passwords are the most common and weak point of ICTs, and it creates serious risks to the organisations. The National Cyber Security Centre (NCSC, 2019) published analysis of the 100,000 most commonly passwords till 2019 that have been accessed by third parties in global cyber breaches. (Figure 1.)

Most used in total	Names	Premier League football teams	Musicians	Fictional characters
123456 (23.2m)	ashley (432,276)	liverpool (280,723)	blink182 (285,706)	superman (333,139)
123456789 (7.7m)	michael (425,291)	chelsea (216,677)	50cent (191,153	naruto (242,749)
qwerty (3.8m)	daniel (368,227)	arsenal (179,095)	eminem (167,983	tigger (237,290_
password (3.6m)	jessica (324,125)	manutd (59,440)	metallica (140,841)	pokemon (226,947)
111111 (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)

Figure1. Most common passwords list done by the NCSC

It shows the most commonly used password revealed in data breaches is "123456", which made up of the first six numerical keys across the top of a keyboard. Many of the topmost are used by over half a million people, being made up a simple series of numbers, repeated multiple times or switching sequences.

Users' own names are also a common password theme, "ashley" and "michael" following by "daniel", "jessica" and "charlie". Meaning that a hacker can crack the victims' emails by only trying their first name.

Moreover, passwords purely based on users' interest could easily find themselves the victim. It's usual to find people sharing their daily lives and interest on social media nowadays, therefore it could be relatively simple for criminals to seek this information out online to crack the account. And the victims mentioned above may be one of the employees in the company, therefore this is one of the risks that the manager should pay attention to.

If failed to do so, organisations' ICTs may be controlled by unauthorised attackers and lead to leak of organisational plans, employees, and customers' data. As a result, loss of competitive advantages, penalty of fail to meet legal compliance, such as GDPR (Voigt, 2017), and liability of contract breaches.

3.2 Potential risk from ICT devices

Some life examples of ICT devices are given in the section. January 2020, a hacker published a massive list of more than 515,000 servers, routers, and smart devices, it includes each device's IP address, along with a username and password. The list was compiled by scanning the entire internet for devices that were exposing their ports. Hackers then tried to use factory-set default or custom usernames and passwords, yet easy-to-guess password combinations. (Cimpanu, 2020) Among these devices, IP cameras especially, are the easy target to access externally and not exclusive to hackers.

Based on my research, I tried to use Google hacking database (GHDB, https://www.exploit-db.com), which is a categorised index of vulnerable web applications, servers, and online devices, to find IP cameras with security holes. After inputting the advanced operators "intitle:"webcam 7 inurl:'/gallery.html"' I got in GHDB, I found 119 results of online cameras, each link could have up to 4 or 12 channels, with multiple views and even allow to be adjusted angles. (Figure 2.)

Figure 2. Examine connecting to IP camera using GHDB

While the IP camera security in personal residence is unsecure, organisations one is equally vulnerable. As organisations' devices are all connecting to the same network, cracking down a device with weak password is like paving a way to the whole system. Nearly one in four organisations relied on same password for all cameras from the same manufacturer, giving hackers easy access into the network once one camera has been compromised. (Genetec, 2019)

IP cameras came with default security settings, including admin login information that is often publicly available on manufacturers' websites, example such as Vacron online camera has default username as "admin" and password as a space. (Figure 3.)

It is critical that organisations should be proactively updating their physical systems and their IT networks with strong password and admin confidential. However, government and organisations with older equipment may not have executed the updates

in practice, and potentially compromising other critical data and systems in the network. (Chevalier, 2019)

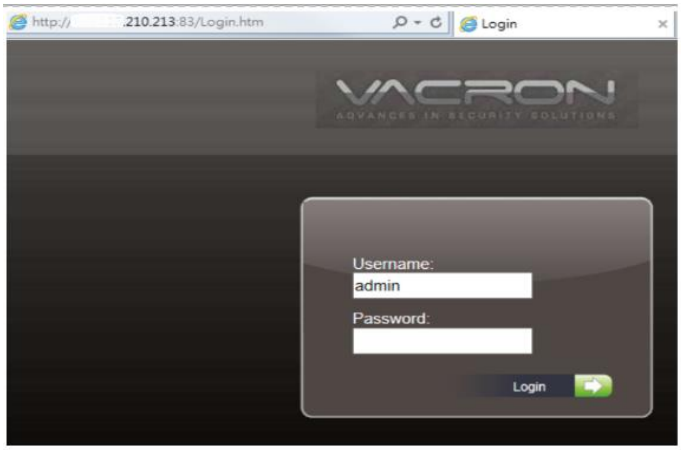

Figure 3. The default Username and password for Vacron online camera

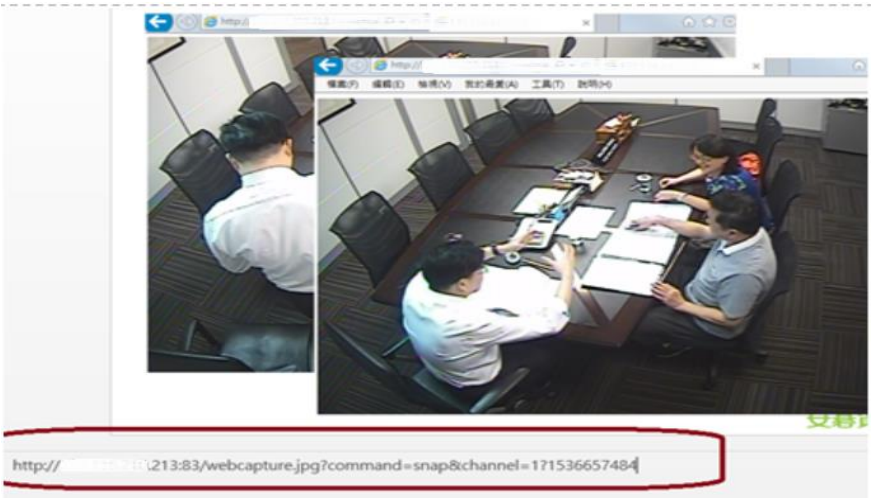

Figure 4. Remotely monitor an office

Figure 5. Monitor IP cameras in factories

Organisations leaking the office camera footages remains prevalent and compromise to their strategy plans and product confidential. It's essential for managers to be aware of these breaches that are putting an entire organisation's security and customer's privacy at risk.

3.2 Incapacity to continue operations due to a deliberated attack

The risks mentioned above are not existed individually, each threat may be the cause or ramifications of each other. That is to say, IP cameras are common devices in office and have been shown widely vulnerable to simple hacks, meaning once it is taken over by the hacker, creating "botnets" by collecting humongous zombie computers and networking them is the next step, so they can all be controlled at once for malicious acts. Botnets bog the system down or use a lot of system resources, and since they have extremely small footprint, it's difficult to recognise when the machine is being used by outsiders, such as spam or DDoS attacks.

A French cloud computing company, OVH, has been subject to a tremendous DDoS attack, which was the biggest attack that ever-taken place in 2016, with peaks to 1Tbps of traffic.

The attack lasted from 16th to 22nd September, these botnets are made up of 145,607 unprotected online cameras mostly from UK, and 25,000 CCTV cameras was used to initiate significant attacks across the world. (Parkin, 2019)

It's unclear where the hackers hail from, the majority of traffic in the latest attacks has come from Asia, particularly China, South Korea, Taiwan and Vietnam. The attack shows a red flag to organisations' security and the management of ICTs, which are the main reasons the attack was taken place. (Brewster, 2016)

3.3 Change Management for organisations

These risks lead to loss of reputation, and lost customers, all leading to lost business. There are few ways to change the way managers manage ICTs (US FTC, 2013) with three stages in Change Management:

3.3.1 Inform & Educate

Inform the employees why prevent these risks are imperative and why the change is taken place. Educate them how the change will impact and how it affects their working.

1) **Secure Internet and Wireless Transmission**

   A good wireless security protocol helps secure the data transmission through routers. Manager and employees should look for devices that support wireless security protocols, like WPA2 and WPA3, and encrypt information, including usernames, passwords, and live feeds using SSL or TLS to protect the information when transit

is imperative.

2) Use stronger passwords

Employees should use stronger passwords but default ones.

3) Set level of access

Levels such as, separate settings for administrators, who have the rights to change passwords, and lower-class management can only access to monitoring. This clarifies the responsibilities and prevent suspicious outsider.

3.2.2 Commit

As the change is fully accepted and gradually become the culture of the organisation, there are more procedures need to keep in mind after informing and educating employees.

1) Keep the software up to date

The system or software that comes with the device needs occasional updates. Managers should make sure periodically update their firmware to fix security flaws and enhance product performance.

4. Conclusion

ICTs enable organisations to work efficiently and gain better competition position in business. However, risks along it in deploying, such as security breaches cause by weak passwords and rarely update firmware, are challenging for managers. One way to react is to adopt change management for approaching new change, ensure the secure of the transit channel and restrict user level access. These risks are only the tip of the iceberg, it's imperative for managers to acknowledge the challenges and educate employees to react seamlessly to the problems may occur.

5. Critical reflections

5.1 More than Change Management - PDCA(Plan-Do-Check-Act)

PDCA, is a continuous loop of planning, doing, checking, and acting. The model allows managers to continuously test what needs to **change** while mitigating risk. It is an alternative aspect for change management.

If organisation wants to improve the stability of its security system, the four stages may be as following:

Plan

Mapping out the ideas to solve a problem, and define the vulnerabilities in the ICT system, collect relevant data or experience from experts and alliances, such as Cloudflare, G4S Plc.

Do

It's essential to train and empowering the people who will have to act, who put things into practice. Things to implement for instance, the regular renewal of the operation system, install anti-virus software and firewall, periodically backup the critical information and data, and turn off unnecessary servers for external access.

Check

Confirm the results through before and after data comparison, check whether the implements have decreased the loss of the attack and removed the vulnerabilities.

Identify problematic parts of the current process and eliminate them in future. Analyse and find cause of the problems. If something went wrong during the process and adjust the plan and go through the cycle again with an ameliorate plan.

Act

Document the results, inform others about the changes. Managers should be aware that PDCA not a process with a beginning and an end, given that the business environment is unpredictable, and improve process based on what have learned in previous stages. If the plan turns out successfully, then they need to standardise the process and implement it across the business and continue to look for ways to improve for organisation.

To sum up, PDCA is an iterative process, four-stage approach for continually improving processes, products or services, and for resolving problems. It involves systematically testing possible solutions, assessing the results, and implementing the changes. It's a process that can be approached along with change management.

5.2 Legal Challenges: General Data Protection Regulation

General Data Protection Regulation (GDPR) is a framework of law requires business to protect on European citizens data privacy in the European Union (EU) and the European Economic Area (EEA) in 2018. It boosts consumer rights regarding their data and sets new standard for companies to be cautious and responsible for it.

Equifax was fined £500,000 for failing to protect their customers' personal information, including names, birth, passwords, addresses, driver license, and financial information, that affects 15 million UK residents by the 2017 cyber-attack.

Uber also was hit with a £385,000 fine after a cyber-attack taken place and the hacker stole personal details of 2.7 million customers and drivers in the UK. Uber paid the hackers £100,000 to destroy the data they downloaded but did not inform the incident

to the affected customers for more than a year. (Macaulay, 2020)

The fine is based on the size of the breach, how sensitive is the information and how the company respond and react to the incident. GDPR is a serious regulation that ensure personal information is protected by the companies, therefore, it's imperative for organisations to understand their responsibility to protect customer data and as well as make right acts to prevent breaches.

Bibliography

1. Ames, A., Stannard, J., Stellmacher, D. (2019). *UK Cyber Survey Key findings – General public*. 1st ed. [pdf] United Kingdom: Ipsos MORI Social Research Institute. Available at: https://s3.eu-west-1.amazonaws.com/ncsc-content/files/UK%20Cyber%20Survey%20-%20analysis.pdf [Accessed April. 2019]
2. Brewster, T. (2016). *How Hacked Camera Are Helping Launch the Biggest Attacks the Internet Has Ever Seen.* [online] Forbes Available at: https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#5ffaf2325899 [Accessed 25 September. 2016]
3. Cukier, M. (2007). *Study: Hackers Attack Every 39 Seconds.* [online] A. James Clark School of Engineering. Available at: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds [Accessed 7 February. 2007]
4. Cimpanu, C. (2020). *Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices.* [online] ZDNet. Available at: https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/ [Accessed 19 January. 2020]
5. Chevalier, M. (2019). Personal interview. *Outdated firmware could be putting IP camera security at risk.* [online] technology Decisions. Available at: https://www.technologydecisions.com.au/content/security/news/outdated-firmware-could-be-putting-ip-camera-security-at-risk-994422321 [Accessed 10 December. 2019]
6. Genetec, (2019). *New Genetec research shows almost 4 in 10 security cameras can be at risk of cyber-attack due to outdated firmware.* [online] Available at: https://www.genetec.com/about-us/news/press-center/press-releases/new-genetec-research-shows-almost-4-in-10-security-cameras-can-be-at-risk-of-cyber-attack-due-to-outdated-firmware [Accessed December 5, 2019]
7. Macaulay, T. (2020) *The biggest ICO fines for data protection and GDPR breaches.* [online] CSO news. Available at: https://www.csoonline.com/article/3518370/the-biggest-ico-fines-for-data-protection-and-gdpr-breaches.html#slide10 [Accessed 16 January, 2020]
8. NCSC, (2019) *Most hacked passwords revealed as UK cyber survey exposes gaps in online security.* [online] Available at:

https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security [Accessed 29 April. 2019]

9. Parkin, C., Rene. Personal interview, September 26, 2019. *OVH suffers 1.1 Tbps DDoS attack*. [online] SC MEDIA Available at: https://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/1476220 [Accessed September, 2019]
10. US Federal Trade Commission, (2013) *Using IP Cameras Safely*. [online] Available at: https://www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely [Accessed 3 August. 2013]
11. Voigt, P., von dem Bussche, A. (2017) *The EU General Data Protection Regulation (GDPR).* 1st ed. [e-book] New York: Springer International Publishing, p.9-30. Available at: https://link.springer.com/book/10.1007/978-3-319-57959-7#about [Accessed 10 August. 2017]