The bare necessities of 'ICT life' for any business

Christopher Jones, PGDip Adv. Net (Open)
Coderz ICT consultancy and tutoring, United Kingdom

Aim

It is anticipated that most people will be able to find some benefit in this paper, however the content is focused on:

- Owners of businesses utilising technology.
- Senior employees involved with policy and technical administration of businesses that use technology.

Abstract introduction

No business is perfect.

Even the most secure, locked down businesses may lose custom based on the way they advertise, promote or display their information.

Equally, if the business isn't available or able to take orders or offer support at all times of the day and night, then there is a likelihood of missed sales.

The purpose of this article is to consider these points and to offer suggestions to increase relative effectiveness and efficiency.

Being secure

Often businesses (of all sizes) lack in their security in one way or another, be it logical, physical or administrative. No business has it all perfect.

Organisations such as *'The International Information System Security Certification Consortium - (ISC)²'*, have built models, principals and concepts around exactly these 'layers of security'. A common model used is the CIA (Confidentiality, Integrity and Availability) Triad, the concepts within this model are simple:

- Confidentiality: To ensure that only the individuals authorised can access and edit the data.

- Integrity: To ensure that the data has not been compromised in transit, by an attacker, or accidentally.
- Availability: To ensure that the data is available 100% of the time it should be available.

These concepts do not apply to a single security layer, in fact, to achieve true security, practices and standards should be applied on a multi-layered basis:

- The physical security layer - This layer is probably the most substantial, if an attacker is able to access physically equipment then they can affect Confidentiality, Integrity and Availability of data.
- The technical/logical layer - Here are technical mechanisms enabling the mitigation of attack, this may include software system hardening, firewall application and use.
- The administrative layer - This layer comprises the enforcement of policy and training. There would be no security issues in ICT without the interactions of human beings, this layer is a way of applying counter-measure methods to humans. These may include:
    - Training and education.
    - Security policy.
    - Acceptable use policy.
    - Rules, standards and guidelines.
    - Appointing technical roles based on job type.

Moving forward into the next generation of networks, including cloud based solutions, IPv6 (Internet Protocol version 6) and the 'Internet of Things' (IoT) logical borders almost become non-existant. Borderless networking provides a difficult challenge for security professionals, as the only really affective place to apply security mechanisms is on the end devices.

There is a lot more to being secure than the ideas mentioned in the extract given, however, the points and concepts mentioned should offer a good start for investigating further measures to increase the security of their business.

Ensuring confidentiality, integrity and availability requires careful planning, employing a security specialist to help through this planning stage is highly recommended and to pay for periodic outsourced penetration testers, to ensure the system remains secure and intact.

Being available

It is essential for many reasons for a business to be available as much as possible, ideally 24 hours a day. Under construction notices, or coming soon promises need to be a thing of the past. The customer has no interest of what is available to them 'two weeks from now'. If they can't access it right now, they're look for an alternative business that can offer it.

Don't make unachievable promises or goals regarding content, products or services.

If features such as answering machine messages are used then it is important to make sure they are inviting, and ensure that the customer is contacted as soon as possible.

Being accessible

What would be the point in an advert that no one could read? The sentiment also applies if only some people can read it. It also applies to services and products, and just about everything written down or 'accessible'.

There are many sites that 'bog you down' with too much information, difficult to read information or just outright obfuscated information.

A great example of this is my use of the word obfuscated, not everyone will understand it, or be able to access a definition easily. Notice that a modal pop-up appears when the word is clicked giving an immediate definition. This allows this document to be accessible to a larger range of individuals, perhaps people with English as a second language.

How many languages, as a business is appropriate to transmit information?

If the aim is to sell something, announcing the fact is necessary, to everyone and anyone in the market, or perhaps even outside it.

Be polite and clear, it is very off-putting to a client or potential client to be greeted an abrasive or standoffish attitude. Taking the time to ensure that the end-user of services is able to feel comfortable about using a company is another abstract form of making business accessible.

In Summary

- Be secure - Follow best practice and up-to-date information security standards, employ professional services, even as a security professional, having a third party double check configurations and policy is strongly advisable.
- Be Available - Ensure that, in some form the business is available 24 hours a day, even if it is with the promise of returning a call. It may be useful to envisage a business from the perspective of the customer; how should they be treated? If the business can afford it, employ third party call handlers, but make sure they adhere to the standards of the business.
- Be accessible - Ensure businesses reach everyone they should. If a potential market is Wales, then bi-lingual data throughout is important.
  Screen readers do not flow nicely on many business websites, because of this, it is difficult for individuals who use text to speech products to access the services, ultimately this may put off potential customers. A screen reader such as Narrator, ChromeVox or NaturalReader may be a useful tool for businesses to test for their own level of alternative access.

References for further reading

- Stewart, James M, Mike Chapple, and Darril Gibson. *CISSP Certified Information Systems Security Professional Study Guide, 7Th.* John Wiley & Sons, 2015. Print.
- W3.org. (2005) *Introduction To Web Accessibility* [Online] Available at: https://www.w3.org/WAI/intro/accessibility.php [Accessed 25th September 2016]
- Dogulin Digital. (2013) *6 Reasons Why A Website Is Important For Your Business*. [Online] Available at: http://dogulindigital.com.au/importance-of-website-for-business/ [Accessed 26th September 2016]
- Cisco Systems Inc. (2010) *Borderless Networks Architecture: Connect Anyone, Anywhere, On Any Device* [Online] Available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/BNArchitecture.pdf [Accessed 29th September 2016]
- Kobie, N. the Guardian, (2015) *What Is The Internet Of Things* [Online] Available at: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google [Accessed 29th September 2016]
- Sans.org. (2014) *Securing The Internet Of Things Survey* [Online] Available at: *https://www.sans.org/reading-room/whitepapers/covert/securing-internet-things-survey-34785* [Accessed 29th September 2016]

Glossary of terms

- Screen-reader – Reads text out loud from the computer user interface.
- ChromeVox – A 'screen-reader' extension for Google Chrome.
- NaturalReader – A standalone text-to-speech software.
- Narrator – Microsoft windows built in screen-reader software.
- Obfuscated – Made obscure, unclear, or unintelligible.
- C.I.A. Triad – A security concepts model used by $(ISC)^2$.
- Accessible – Able to be accessed, read, or reached.
- Logical – For the sake of use in this article is used to mean technical through software.
- Physical – Any physically tangible object or environment.
- Tangible – Accessible by touch.
- Administrative – 'Relating to the running of a business, organization'
- Borderless networking – networks that do not have logical boundaries,
- IoT (Internet of Things) – the collection of dumb and smart objects into interconnectivity.
- End devices – Computers, printers, tablets and devices used by the end user.
- Hardening – Employing software and hardware methods to improve the security of a device or network.
- IPv6 – The next generation of internet addressing. Each and every device will have its own IPv6 address, so many security mechanisms will be a think of the past and devices will be far more easily accessible.