Metaluxo IT Security

Essentials to keep your business running in the data breach era.

"65% of consumers unlikely to do business again after a data breach"

-SafeNet Survey July 2014

Your Business is at Risk

Cyber-security might be only one component of your business strategy, however, it can be a critical one if you do business mainly online. Large organisations are investing heavily in cyber-security defences, however small organisations are still lagging behind and cybercriminals are taking advantage of this fact.

Many governments around the world are taking steps to bring Small & Medium Enterprises (SMEs) up to date with information security. The European Commission estimates that 99% of the businesses the European Union are Small & Medium Enterprises and are a key driver for growth in Europe[1].

What do they want?

Many businesses consider that their information is not valuable enough, or that they are not very important to be target of hackers. This cannot be farther from reality. Cyber-criminals are increasingly pointing to startups and small businesses which are easier to hack and usually do not have proper defences to even detect this attacks. There can be a number of reasons to attack your business online:

- **Financial gain.** Getting the payment details of you or your clients is very profitable in the black market. E-mail addresses and physical addresses are also sold for a profit.
- **Activism**. People with a cause can try to cause disruption to your business because of the nature of your business or simply because of your location or political affiliation.

[1] Entrepreneurship and Small and medium-sized enterprises (SMEs) http://ec.europa.eu/growth/smes/index_en.htm

- **Testing**. Many people see as a challenge to break-in online in any website. Your business might not have any particular reason to be a target, they are just looking for a testing ground.
- **Business advantage**. Competitors (even in other countries) might want to diminish your business capacity by harming your online activities.

Why the need of cyber-security for you?

Regulatory compliance across Europe has strict requirements for data privacy and security. Besides that, more business partners are requiring proof of adequate information security practices and, more importantly, clients are more aware of data security and demand keeping their information secure.

Moreover, the destructive nature of data breaches can bring an entire organisation down. It is calculated that around 65% of consumers will not do business again at all after a data breach becomes public.

Many banks and insurance companies also require proof that appropriate measures were taken to protect company's information before paying for losses.

Most recently, Google is ranking better those websites that have implemented SSL [2].

What you can do right now?

Most of the small companies have a limited budget. However, even with constrained resources there is a number of steps that can be taken in order to protect your information:

[2] HTTPS as a ranking signal http://googlewebmastercentral.blogspot.com.tr/2014/08/https-as-ranking-signal.html

Basic Protection

This is the very basic protection baseline that you need to adopt for your small business. Use the following checklist as a guideline:

- **Download software updates.** As incredible as it sounds, many organisations are running in outdated operating systems (Windows XP for example) or software which has never been updated. You need to adopt a policy to keep up with the latest patches and updates. If you're unsure about this, ask your IT department to teach you how to this yourself and automate as much as possible. Personal firewalls and antivirus should also be kept up to date.

- **Use strong passwords and a password manager**. Many SMEs are using cloud services. However, using weak passwords and repeating them everywhere are one of the main sources of risk for small businesses. Remembering too many passwords is impractical, one solution is to use a password manager such as LastPass.com.

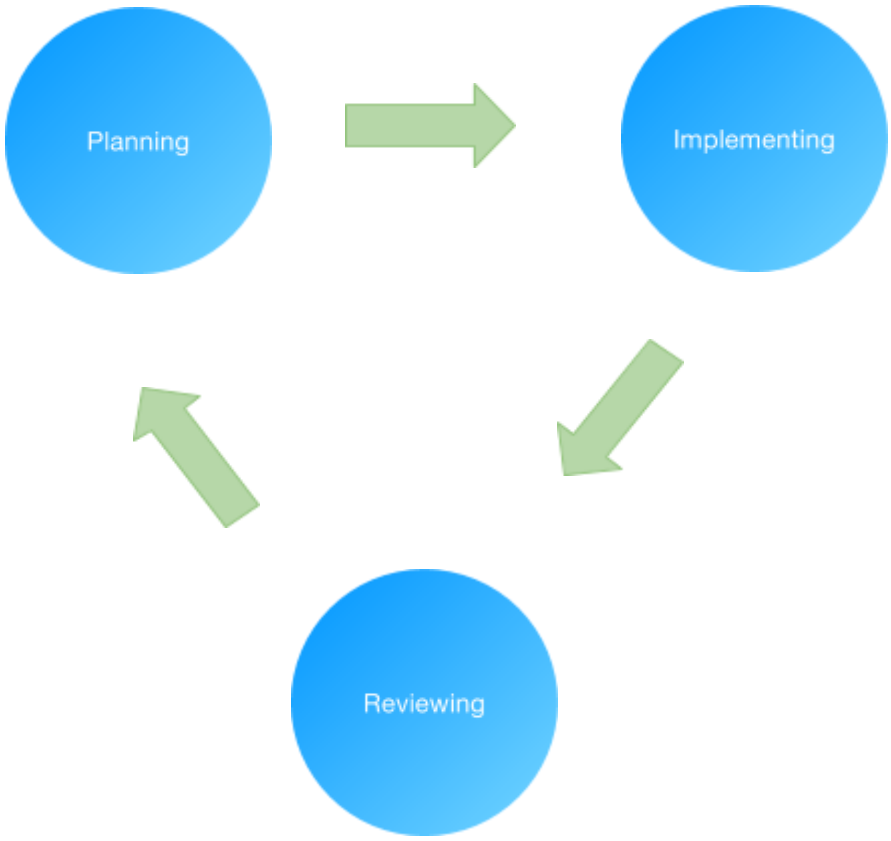
- **Encrypt your devices**. Using a password in your computer is not enough. Information stored in there is not encrypted by default most of the time, and it is incredible easy to get this info if someone can get hold of your laptop or your phone. You need to actively encrypt your devices. Android and iPhones have this capability now, and there is a number of options for your laptops.

- **Delete dangerous e-mails and attachments**. Avoid running macros by default and be suspicious of any e-mail even from known sources. Downloading and opening attachments are specially dangerous.

- **Train your staff**. No single piece of technology will help you if your staff is not aware of cyber-security practices. Most small businesses cannot afford full trainings, however there is a number of free resources that can be used. Online trainings by a specialised company is also an option. See training as an investment, not as an expense.

Risk Management

Managing risk in your business is the key to keep one step ahead of cyber-criminals and minimise IT security issues.



Planning.

These steps will help you to implement information security as an integral part of the business.

- **Determine the likelihood of an attack**. Check with similar companies in your area and check your industry sector for risk levels.
- **Identify governments and business regulations that you need to comply with**. For example the EU Data Protection Directive or PCI-DSS. Consider where is your data stored, there are restrictions about storing personal data outside of the EU.

- **Check with your insurance provider to know if it covers cyber-security attacks**. You might need to have a minimum level of security for your security policy to apply.
- **Assess which information is the most critical for your business**. Client information, credit card numbers, addresses, and other financial and personal information are common targets.
- **Identify your critical IT systems**. Usually your e-commerce website, your CRM and your databases are the most critical IT systems.
- **Identify critical third parties**. For example your payment gateway or your hosting company.
- **Identify critical hardware**. Consider what happens if you lose your laptop or phone. How much personal and customers' information is held in there?
- **Plan for the worst.** What happens if you lose internet connection, your database is breached or an employee tries to commit internal fraud?
- **Identify the level of IT security awareness of your staff**. Even IT staff might not have the correct level of awareness.

Implementing.

Put controls to mitigate your risk. Consider as well third parties, now that many services are in the cloud, consider their location, their data protection levels and any relevant Service Level Agreement.

- **Malware protection**. Keep up to date your systems, including mobiles and tablets, and install a reputable anti-virus. Keep the latest definitions up to date. Do not fall victim of the myth that some platforms like Mac OS X are not susceptible to viruses. Install a personal firewall or enable it in your operating system.
- **Enable two-factor authentication**. Many services such as Google Apps, Dropbox and LastPass allow to use two-factor authentication. This means that besides your password you will need another piece of information such as a code sent via SMS or a one-time password. Many times this can be enabled for free.
- **Protect your networks**. Getting information through your WiFi is a common attack vector. Do not use WEP encryption in your router, use WPA/WPA2 only. Use a

strong, long password. Be careful of open ethernet ports in your office. Have a separate WiFi network for guests.

- **Manage user privileges correctly**. Restrict employees and third parties from accessing personal and business information. Review who is accessing what information and keep it to a minimum necessary. Have a Non-Disclosure Agreement ready for any new employee or third-party.

- **Be careful of removable media**. Train staff to be mindful about USB sticks, restrict their use if possible. Adopt policy to avoid saving personal information on removable media. Give personnel encrypted USB memory sticks to use.

- **Protect your website**. Have a professional to review and harden your website, disable unnecessary services and have strong password authentication procedures. Encrypt as much information as possible on your website. Use web-application firewalls solutions such as the free service of CloudFlare.

- I**nstall an SSL certificate on your site**. This not only protect any information you interchange with your clients, but also give confidence to potential customers, third parties and give you some Google boosting.

- **Be mindful of social media**. Train staff to avoid sharing too much information on social media, monitor social media channels for possible data disclosures or hacking attempts.

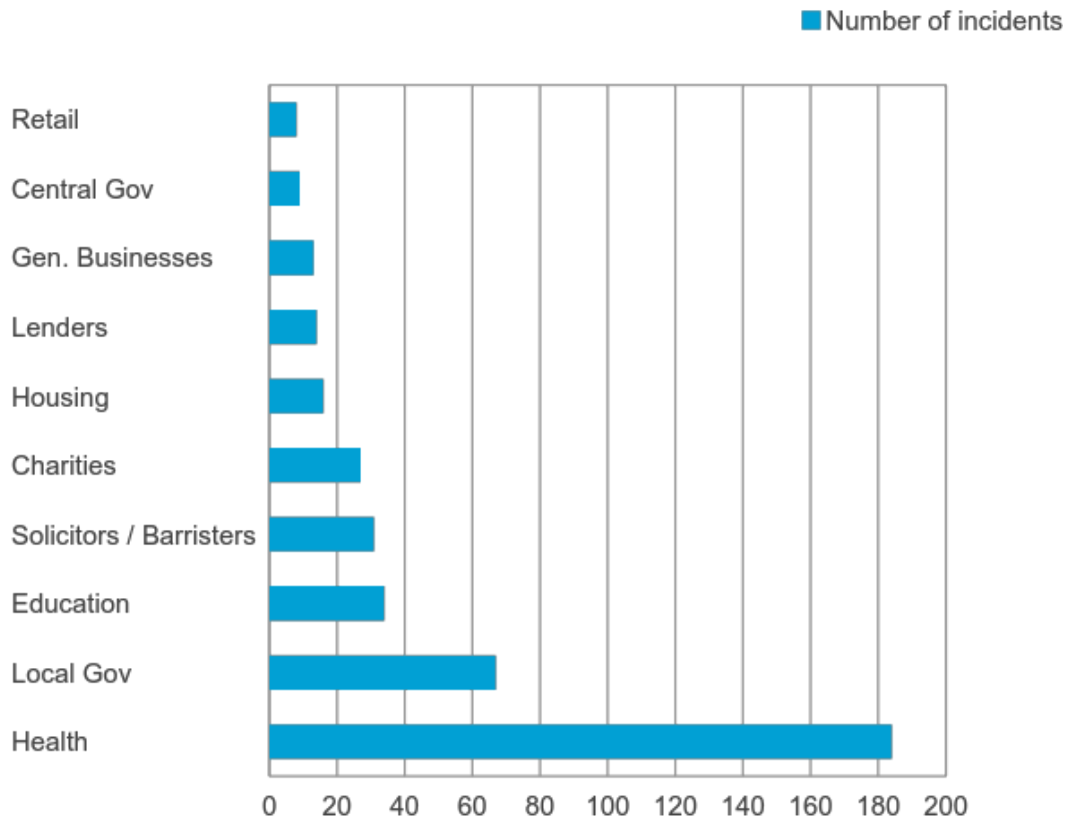


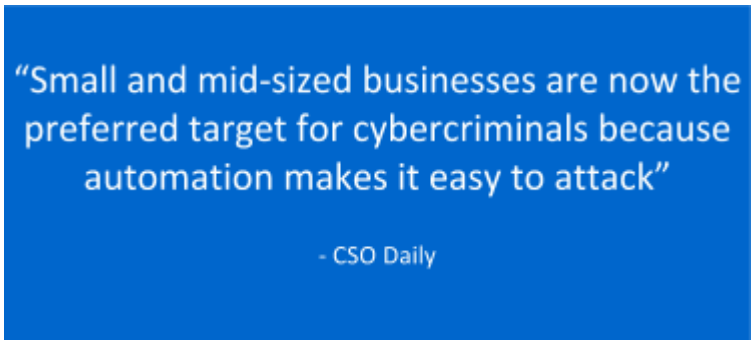
Chart 1. Cyber-security incidents by sector 2014. Source: UK Information Commissioner's Office.

Reviewing.

Your information security policy is not static. You need to continuously check if the planning and implementation phases are relevant for your business. As your organisation grows, third parties are added or your structure changes, your policies have to change as well.

- **Test and re-test**. Once you have a policy and controls defined, test them! Switch off the router in the office and test your Business Continuity Plan.
- **Review the logs**. Check what the logs are giving you and identify possible threats stopped by your measures.
- **Review your policies**. Have a schedule to review your policies and controls after an incident and on a periodic basis.

- **Join free Small Business communities.** This is a way to get up to date information about cyber threats. For example https://www.cyberstreetwise.com have useful information for free, even if you are not in the UK.



3

Audit

Having a security policy unfortunately is not enough. You need a trustable third party to help you review and audit your policies and systems. Many times Small Businesses are unable to afford the fees of a consultant, however, there are at least some strategies that you can do for auditing:

- **Have a fellow business review your policies**. They need to be trustable enough and have an NDA signed. You can review their policies in exchange as well.

- **Have an IT security intern to do it.** It might not be at the level of a professional service but many postgraduate students of IT security are keen to gain field experience and give you valuable insights for free. Anyway, make sure to do your proper checks on new personnel!

- **Check with your local business chamber**. Many times some experts can give you free or low-cost advice as part of a training or conference.

[3] Why Criminals Pick on Small Businesses
http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html

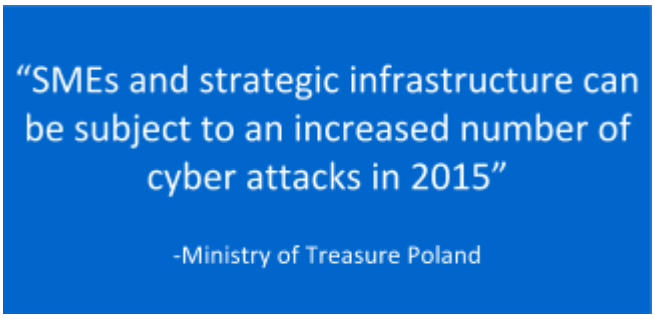
How we can help *Your Business*?

Metaluxo IT Security can help you to protect your businesses success in different ways:

1. **Working with your IT team to protect your client's data**. This includes vulnerability assessments, penetration testings on your app, helping you with SSL certificates and securing cloud services you might use such as Gmail, Salesforce or Dropbox.

2. **Helping define an IT policy.** We will do a Risk Analysis and work with your stakeholders to determine risks and how to address them. We have two main options:
   a. We do the initial draft, train you about risk management and you finish it and review it. We can give you ongoing support. This option is more cost-effective although it requires more work on your side.
   b. We can do a more in-depth business study to determine and address your risks, tell you how other players in the industry are managing them and train your staff to continue improving the policies. This option might be more expensive, however will delivery faster results.

3. **Training your staff.** We can tailor training plans specifically for the skills of your staff. This can be delivered online or on-premises. We provide recordings of the trainings and all training materials so you can re-train additional staff later on.



[4]

Please contact us on hello@metaluxo.com to discuss your particular IT Security needs and get an obligation-free quote.

[4] Risk of Cyber Attacks on Polish SMEs on the Rise
http://msp.gov.pl/en/polish-economy/economic-news/6053,Risk-of-cyber-attacks-on-polish-sme-on-the-rise.html

About Metaluxo

Metaluxo IT Security is the front name of a group of professionals giving advice and offering strategies to small and medium businesses in Europe and abroad about their cyber-security strategies. The company was founded in 2012 in London in order to help small organisations and startups to protect their IT systems, a segment of the market traditionally neglected by larger IT Security firms. In 2013 Metaluxo IT Security became an Affiliate Partner of DigiCert one of the largest Certificate Authorities on internet.

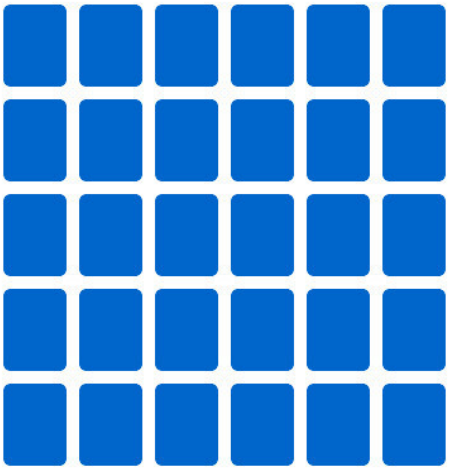
Roberto Arias, MSc (roberto@metaluxo.com), Senior IT Security Consultant. Roberto has worked in the IT industry for more than 12 years. He holds a Master's Degree in IT Security by Macquarie University, advanced qualifications in Policing, Intelligence and Counter-Terrorism and is a Vulnerability Management Certified Specialist by Qualys. He has been working for a variety of companies the United Kingdom, Germany, Australia, Singapore and Mexico.
Languages: English, Spanish.

Katarzyna Bednarz, MA (katarzyna@metaluxo.com), Client Success Manager. Katarzyna has over 10 years of professional experience having worked in high-profile IT security companies such as Thales and RSA and a variety of organisations in the United Kingdom, Germany, Spain, Poland and the Czech Republic. She holds a Master of Arts in Political Sciences and Languages by Dresden TU and Universidad de Granada.
Languages: English, German, Polish, Spanish.

Alfonso Arias, BSc (alfonso@metaluxo.com), Associate Consultant & Business Development Lead. Alfonso has over 15 years of experience in different areas of IT in a number of industries in Mexico including the large Oil & Gas conglomerate Pemex. He holds a Bachelor of Science degree in Informatics specialised in Computer Networks by ITVH.
Languages: English, Spanish.

QUALYS® CERTIFIED SPECIALIST

digicert Official SSL Affiliate Partner



metaluxo.com