Specially prepared

LACPA 21st International congress
Phonecia Hotel - Beirut

DEC 04 – 05/2017

Dr Salah A. Rustum
Chairman & President

CIEL / GlobalSign

Table of Contents

2018 Cybersecurity Predictions

what is in store for us in the next year?

- *By the End of 2018, 85% of All Web Pages Will Be Protected by HTTPS*

Chrome has been marking sites that collect passwords or credit cards as insecure since Chrome 56 (JAN 2017) and Chrome 62 (OCT 2017) -> now marks all sites with input fields as insecure.

It's just a matter of time until all HTTP sites are marked as insecure.

- *Expect More Botnet IoT Attacks*

In 2018, we will continue to see exploits of IoT devices with usage aimed at botnet activity. The scope of unsecured devices is still large, which makes low hanging fruit for hackers.

More Legislation, But Not Much Guidance

2018 Cybersecurity Predictions

- *Businesses Will Start to Get More Serious About Cyber-Insurance; Premiums Will Inflate*

  *Cyber-insurance, despite the attacks throughout 2017, will continue to grow at a fairly steady pace despite the awareness being a not **'if' but 'when'** an attack will take place.*

  The catastrophic attacks in 2017 established that cyber-risk is now a prominent threat.

  *Moving Insurance from **'Risk Protection' to 'Prevention'***

- *The Impact of General Data Protection Regulation (GDPR) in the EU*

  2017 has seen the biggest shift in focus within information security for more than a decade: data protection

What Does GDPR (General Data Protection Regulation) Mean for SEO (Search Engine Optimization) ?

The General Data Protection Regulation (GDPR) when it comes **into effect in May 2018**, it will have a huge impact on businesses throughout the EU, including the UK.

Over the coming year, we're likely to see more and more countries striving to equate local laws with those of the EU.

Whether you work with an **SEO (Search Engine Optimization)** agency or do all of your digital marketing in house, it's vital that you should understand how GDPR will affect your company. Here we look at the critical influencing factors within the GDPR that could alter SEO to see what changes you might need to make.

What Does GDPR Mean for SEO ?

❖Implications for Website Goals

One of the most important aspects of SEO (Search Engine Optimization) relate to the goals that you track on your website. It should be recognized, then, that the GDPR can have an impact on tracked goals that you have set up.

Once the regulations come into force (this will be in MARCH 2018) you will need to be explicit on what you will do with a customer's set of data.

This means that you will no longer be able to request someone's email address for a newsletter sign-up in order to send them additional marketing material, unless this has been made completely clear.

❖Managing Consent

Some sites current use a version of the phrase "by using this site you are agreeing to our Cookie Policy" in order to gain consent, however, under the GDPR this will no longer be considered valid and your sites will need to get users to actively agree rather than passively.

What Does GDPR Mean for SEO ?

❖How Will GDPR Affect Analytics?

It will be necessary for every business to consider how they currently use customer data for any analytics process.

Look at your own analytics – you may find that internal processes such as sharing personal data with employees across emails or specific information contained in email marketing reports may contravene the rules.

❖GDPR Compliance as a Ranking Factor

There has not yet been any indication from Google or any other search engine that GDPR compliance will become a ranking factor in their results – but this doesn't mean that it won't happen.

What Does GDPR Mean for SEO ?

❖How Will GDPR Affect UX(User Experience) and Usability?

Increasingly Google and other search engines are using user experience (UX) as a ranking factor in their algorithm.

It is likely that web designers will have to work closely not only with SEO experts but also those with a good understanding of GDPR compliance to ensure that the designs incorporate the necessary features while remaining user-friendly.

One of those features hitting the news lately is SSL. As the general public becomes more security conscious, it is more important than ever for companies to make it clear that their sites are legitimate (i.e. not a phishing or spoofed site) and can be trusted

What Does GDPR Mean for SEO ?

❖Your Next Steps

If you are concerned about how the GDPR will influence your business' Google rankings, it's a good idea to speak directly with your SEO manager or agency.

Alternatively, if you are a small business and you manage your own SEO, it could be prudent to have some form of consultation on the issue to ensure that you comply with Google's rules.

The good news is that Google and other search engines rarely make extreme changes to their algorithms and usually give websites a grace period in order to get up-to-date with best practice.

Your Business Could Lose Up To $15 Million

- It’s one thing to lose money through market or industry fluctuations, but losing money because you forget to renew your SSL Certificate can be disastrous for your company, especially your brand image and trustworthiness with your prospective and existing customers.
- Research shows that nearly two thirds of businesses already admit to having lost customers within the last two years because **they have failed to secure their website with the right certificates.**
- When customers lose trust in your website and consequently your business, they may decide to take their business elsewhere in fear of having their data stolen
- Incident response, settlements, legal fees, fines and PR are just a number of costs that your business may incur because you simply forgot to renew your certificates.

Your Business Could Lose Up To $15 Million

Here's a few steps you can now take in order to make sure your website is secure at all times:

- **Recruitment and resources**

  As an owner or senior level director within an organization, it is likely to be increasingly difficult to pay your full attention to the IT security requirements that are commonly needed.

- **Ensure you are keeping up-to-date with IT security news**

  By regularly keeping up-to-date you can react quickly when new bugs or viruses are reported or updates need to be made

Your Business Could Lose Up To $15 Million

Enforce internal policy

Here's an example of some of the procedures you may want to implement to protect your business both internally and externally on a physical and online level:

- ***Smart card/key*** *job entry access to buildings, offices and rooms, with varying permission levels for different staff*
- ***Company policies*** *to include regular employee training on best practices and how to detect and report potential security threats and issues*
- ***Two-factor authentication*** *for employees to access machines, devices, networks and online portals*
- ***Digitally sign emails*** *to prove authorship and prevent tampering and encrypt emails containing sensitive data and information*

Your Business Could Lose Up To $15 Million

Do an internal audit

Start by bringing together all of your current certificates and keys and looking at where there might be gaps.

If you're a customer at GlobalSign then you can use the ***certificate inventory tool*** *to check where you have already installed certificates and when you will need to renew them.*

Alternatively, you may want to look at having a ***managed SSL*** *solution where you can control your certificates through an online platform and be notified of certificates needing renewal in advance.*

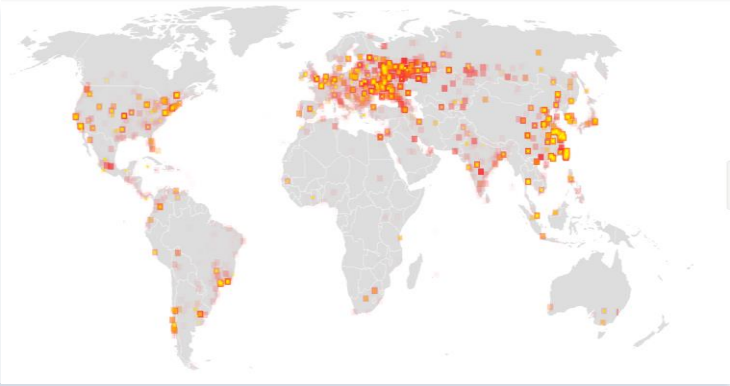
Issues Observed with Industry Practices

the Office of Compliance and Inspection & Examination's (OCIE) Announcement to include Cybersecurity as a key in 2015 examination priority was perfectly timed.

And In accordance with OCIE noted in their 2017 legislation that

- **First**, many cyber-related policies and procedures were not reasonably tailored to the particular entity because they "provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or were vague" or provided contradictory or confusing instructions.
- **Second,** regulated entities failed to consistently conduct annual customer protection reviews, ongoing security protocol reviews and employee training, even if required by the regulated entity's cyber-related policies and procedures.
- **Third,** regulated entities' Regulation S-P compliance activities were lacking in regular patch management for software systems, replacement of outdated operating systems and remediation of high-risk findings from penetration testing and vulnerability scanning.

2017 has certainly been a busy year for cybersecurity professionals



We've witnessed sensitive data leaks from the National Security Agency, the Wannacry ransomware scheme and of course the massive Equifax breach.

1. The Shadow Brokers (an Elite Hackers) has sporadically leaked sensitive data from the National Security Agency.
2. Wannacry ransomware - More Than 200,000 Computers Are Affected So Far, a deadly "ransomware" which locks your computer and all the files become inaccessible and encrypted.
3. Equifax breach. A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

Setting the Stage

- Privacy, safety, and security are becoming more distinguishing factors in ANY consumer related business and for most industrial applications
- Increased Threats, Compliance Security is key
- The value of your business transactions cannot be realized without the implementation of strict (device) security and identity mechanisms
- Leverage existing technologies to build security and identity into the Organizations ecosystems

What Should You Look for When Choosing a CA?

Picking a Certificate Authority (CA) seems easy enough right

One quick Google search on how to obtain an SSL Certificate for your website or an S/MIME Certificate for email encryption will give you plenty of websites that offer you cheap or even free digital certificates.

I know getting something for free is great…until you run into any issues, that is….

Price is one of the most common deciding factors when comparing CAs, but should it be?

When the security and reputation of your company depends on it, do you really want to just go with the cheapest solution?

What Should You Look for When Choosing a CA?

There is so much more that goes into choosing a CA.

1. **The Platform**
2. **Easy to do Business With**
3. **Support**
4. **Ubiquity, Longevity and History**
5. **Innovation and Automation**

They should have top tier support for not only when things go wrong, but also day-to-day interactions with a knowledgeable account manager who can adapt their products to your specific enterprise needs.

You also want a CA who can grow with you when you're ready and just like any vendor, you want to make sure they'll always be there for you, ready to help.

How Top Industries Are Preparing For Evolving Cybersecurity Threats

- Continual education of security professionals
- To adopt security basics like encryption, authentication, antivirus tools and firewalls.
- Investments in cybersecurity; measures must be taken to replace vulnerable and outdated computer systems.
- Enable secure electronic document workflows
- Meet Compliance requirements on digital signatures
- Ensure document integrity and authorship
- Time stamping services included to support time sensitive document transaction and audit trails
- HTTPS with properly configured SSL/TLS is a must to encrypt the connection with retailer websites and secure all customer transactions.
- Enforcing stricter control and authentication over the software and hardware used.

CIEL LEBANON

GlobalSign GMO Internet Group

THANK YOU