CYBER SECURITY (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/CYBER-SECURITY/)

2016 cyber security predictions: top threats and countermeasures

56 MINS AGO *by* HOWARD SMITH (HTTP://SECURITYGLADIATORS.COM/AUTHOR/HOWARD/)

Potential cyber attacks that could impact you and possibly your business in 2016

With the advancement of technology (http://securitygladiators.com/2015/02/28/technological-growth-creating-more-security-loopholes/), added to the fact that we're becoming more 'digitally' focused. We've dipped into the crystal ball and randomly looked into seven (7) different aspect of life in 2015 (in regards to cyber security and privacy) and what the risk will be in 2016.

Don't expect links to other sources, what we're calling on here is that all readers to take a step back and use common sense. So you won't be just seeing headline articles, as ever we at Security Gladiators are playing the 'devil's advocate'! So, here we go…

Fantasy sports

We proffer that it's exactly that, it's 'Fantasy'. One could spend time talking of huge amounts of either money spent, or even that which 'Cyber criminals' make. Like a lot of things in life, they tend to originate from America, the land of 'Milk and honey', lyrics used in Chris Rea's song 'Looking for a rainbow' from the 'Road to hell' album, then it floats across the pond …..

So what's new, nothing, just like the actions of many users, the harbor of the greatest 'risk' on the Internet? Irrespective, whether talking of 'Billions' or the money which the user wishes to make the 'Millions'!! What's even more valuable here is the personal or sensitive data (http://securitygladiators.com/2015/11/11/protecting-sensitive-data-through-encryption-and-other-means/) that is entrusted to betting syndicates (even those on the black market) without any fore thought.

And so, the data is given in an ambivalent manner, then when all goes 'awry', just like the 'Plans of mice and men', by Robert Burns, is the user up in arms and all is lost. When will people wake up? Risk is a core issue here, it's the users 'risk' of entrusting a third party with their personal information, let alone the money put forward!

Ultimately, there's only one winner (*and it doesn't need rocket science to unveil this*), so what will 2016 bring, fancy a bet, and watch this space.

Presidential candidate

Photo: By DonkeyHotey (2012 Republican Presidential Candidates) [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3A2012_Republican_Presidential_Candidates_caricatures_big.jpg)

The use of social media will be a key factor in the race for the White House (and other parliaments of countries worldwide), just as in many other electoral issues. The power of social media is phenomenal; it will make or break even the best.

Irrespective of which media is used and no doubt there could be even more mediums to choose from by the time the next election is on us. A key factor here is that 'personal' data of the candidates will be used and at 'risk'.

The inevitably of hacking (http://securitygladiators.com/tag/hacking/) will take place, leading to extortion and blackmail, tools of the underworld. The myriad of reports from the like of CIO world, and its counterparts, for some reason people don't read or understand the 'risk'.

Whether a user or potential presidential candidate, failure to understand or take heed of the advice given, we find incredible. Where is people common sense, we'm not talking of rocket science here, it's the basics so what more has to be spelt out?

Planes, trains and automobiles

Photo credit: Michaelberry (//en.wikipedia.org/wiki/User:Michaelberry) at en.wikipedia (http://en.wikipedia.org) [CC BY 3.0 (http://creativecommons.org/licenses/by/3.0)], from Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3ACanada_Line_Skytrain_Cars-2008-04-22.JPG)

The modes of transportation have always been with us, yet the makers have been ambivalent when it comes to 'personal security'. Where is their loyalty to the customer or even potential customers? Or is the race to a higher balance sheet more important, or to be the first in the race to market their new innovations?

We readily ask Cherokee or Boeing, How do you value the life of a human being? Surely, it would be common sense to test your new products before they are released for sale. You must undertake 'Risk' assessments against your new innovations (http://securitygladiators.com/2015/06/20/jaguar-to-monitor-its-drivers-heart-rate-breathing-

and-brainwaves-with-nasa-tech/)? Are your risk metrics released to the public, or are these a company secret? What remediations are taken place and what is the value of your 'Risk acceptance'?

So whether it's a Plane, train or automobile, a key factor (http://www.newsweek.com/future-hacking-your-planes-trains-and-automobiles-arent-safe-350865) here is that the driver/pilot and passengers will be a '**Human Being**'. Advancement in technology will occur, this can't be stopped, it's human nature, but at what cost?

Drones

Photo: By U.S. Air Force photo/Staff Sgt. Brian Ferguson [Public domain], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3AMQ-9_Reaper_taxis.jpg)

With the advancement of technology we now live with 'Drones', a whole new concept of how the will impact on our daily lives. We see in the news of how the Drones are able to monitor operational environments in war-torn countries. Ultimately, we see this use would be perceived in the ultimate role, good or bad, depends on which side of the fence you are.

Though let's not look at the dark side (http://www.ibtimes.co.uk/dark-side-drone-police-reveal-uavs-being-used-theft-smuggling-spying-children-1523662), because they will be positives. In the bigger scheme of things, they will be used for traffic control on roads. But they will be susceptible to intrusion, thus they must have been tested before release into an operational environ.

However, when used by governments or the health industry, a key factor here is their systems robust enough to withstand penetration from drone mechanisms? They are the host to holding personal information, as such are there systems subjected to sound 'risk' and penetration testing processes?

They will be honeypots for the cyber criminals to exploit. Personal data will be freely given by members of the public in the nature that it will be protected. However, we see how this type of data is vulnerable when in the hands of employees, let alone the threat from drones, thus increasing the 'risk'! Will 2016 see better protection?

Major sporting event

Photo: By Stefan Bellini (Own work) [CCO (http://creativecommons.org/publicdomain/zero/1.0/deed.en)], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3ADamaged_Hard_disk_drive_for_data_protection_.JPG)

We've seen already in 2015 Russia banned (http://www.dailymail.co.uk/sport/sportsnews/article-3311082/Russia-banned-Olympics-one-Russian-athlete-competes-summer-sport-lost.html) from the Olympics for drug testing in previous Olympics. Therefore tampering with timing machines is not beyond possibility, unless robust systems are in place to preclude such activity.

It's obscene that those external to athletes could consider this type of activity, but the cyber criminal has no morals. For them, tampering with race results in order to achieve a higher prize in monetary value is the golden chalice. Of course one doesn't have to be at the same scale of the Olympics, it could be the European championships.

Irrespective of how they are penetrated, the tools have been used for years and fine-tuned in order to make them more robust. Surely, it's about the pure enjoyment that millions of the public gets from viewing such events. When Russia was exposed this year, immediately I thought of past

Olympians who came 4th, have they been equally recompensed, but what about the moment when they should have stood at the medal presentation, viewed by millions, which will never be recreated. The loss is beyond words!

Thus the attention to the detail is critical, whether on the corporate basis or by the individual, 2016 would undoubtedly be see more risks lurking, whether technical or personal, diligence must be of the highest order.

Mobile Malware

Photo: By www.elbpresse.de (Own work) [CC BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3AVirus-Meldung_mit_Lupe.jpg)

Predictions are like the weather forecast, same old, same old!!! There has been a definite shift from desktop to laptop, more of late the shift is towards mobile devices and let alone the BYOD and their security (http://securitygladiators.com/2015/03/02/prevent-byod-security-breaches/) (*how I hate this acronym and what it stands for*).

Get things back in house is our team at Security Gladiators' motto, maybe we're and aging old school type. This said, we view the whole thing governed by 'risk' and the user can be quite ambivalent when it comes to 'risk'. This is even more so when it comes to Personal Identifiable Information (PII) (https://en.wikipedia.org/wiki/Personally_identifiable_information). If the individual wants to take the risk with their PII, that's fine, but surely not when it's others PII and a BYOD device is being used, that's too much.

Money isn't worth it, more so when individuals' personal identities are then placed at 'risk'. When someone wants to buy a new device, this becomes their focus, as they will be the envy of the office. But do they then think of how they will then transfer the data to their new device? Have they then considered about how they will expunge the images from their old device?

Maybe 2016 is worthy to take a step back and think what they're doing and what they're playing with?

3rd party attacks or data destruction

Photo: By Stefan Bellini (Own work) [CC0 (http://creativecommons.org/publicdomain/zero/1.0/deed.en)], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3ADamaged_Hard_disk_drive_for_data_protection_.JPG)

Either one of these issues, by implementing ISO/IEC 27001 and getting certified would be a positive step forward. The Management System under 27001, allied to the Codes of Practice (COP) under ISO 27002 (https://en.wikipedia.org/wiki/ISO/IEC_27002) is a means to address both.

Control 7.1.2 is the core means of addressing Data Protection, this further supported under the Controls of 18.1.2 Intellectual Property Rights and 18.1.4 Privacy and protect of personal identifiable information. Both are intrinsic to Data Protection.

One aspect that people tend to miss is the destruction of hard copies of documents. In today's society, people also fail to consider the images of documents, more so when equipment is going for destruction. Thus, it's imperative to ensure the right process is in place to destroy paper and disc drives. Certainly in the UK (if you take UK alone as an example here), the Information Commissioner can fine up to £500k for failing to comply with the Data Protection (http://securitygladiators.com/2014/08/16/protect-online-data/) Act.

The control in the life cycle of all media is accurately covered in Control 8.3 for all aspects.

Now 3rd Party attacks could be controlled by having a penetration testing regime, regularly policed and documented. However, there are those 3rd parties which will form part of your normal working practice.

In order to protect you, best practice will indicate that by taking time at the outset will ultimately protect the business. Equally it would be provident to review the functionality of 3rd Parties, are they providing what you are paying them for? Can you trust them? These are important questions that you will need to have answered before entering into a contract.

Under Control 13.2.4 Confidentiality or non-disclosure agreements are a good way in ensuring any 3rd Parties know that you mean the real business. The whole area of Control 15.4 is relative to 3rd parties and their impact to security supplier relationships.

NEXT ⌄ TOP ⌃

As a parting shot here, always remember the 'Target' debacle of 2015!!

Conclusion

Whatever sphere you're working in, give thought to the medium and what's at stake. Ultimately, there will be your personal data and that of others, but what ownership do you apply? What 'risk' do you apply? Maybe for 2016, make 'Risk' and 'Ownership' be the first entities you review.

Have a good festive season, and may 2016 be in your favour.

Top/ Featured Image: By Andersson18824 (Own work) [CC BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons (https://commons.wikimedia.org/wiki/File%3ASyrian.hacker.jpg)

Subscribe or Follow

Stay informed, stay safe! Get information and guides on online freedom tools, web anonymity, alongside unbiased security reviews and latest happenings in the world of cyber security.

email address

Subscribe

(http://securitygladiators.com/feed/) Subscribe to RSS Feed (http://securitygladiators.com/feed/)

G+1 76

Like 231

Follow 335 followers

TAGS: BUSINESS INSIDER (HTTP://SECURITYGLADIATORS.COM/TAG/BUSINESS-INSIDER/), BYOD (HTTP://SECURITYGLADIATORS.COM/TAG/BYOD/), CYBER ATTACKS (HTTP://SECURITYGLADIATORS.COM/TAG/CYBER-ATTACKS/), INTERNET SECURITY (HTTP://SECURITYGLADIATORS.COM/TAG/INTERNET-SECURITY/), PERSONAL INFORMATION (HTTP://SECURITYGLADIATORS.COM/TAG/PERSONAL-INFORMATION/), SECURITY PRACTICES (HTTP://SECURITYGLADIATORS.COM/TAG/SECURITY-PRACTICES/), SECURITY RISKS (HTTP://SECURITYGLADIATORS.COM/TAG/SECURITY-RISKS/)

HOWARD SMITH (HTTP://SECURITYGLADIATORS.COM/AUTHOR/HOWARD/)

SERVED IN THE ROYAL AIR FORCE (RAF) FOR 30 YEARS IN THE TELECOMMUNICATIONS TRADE. WHILST IN THIS ENVIRON, DATA COMMUNICATIONS WAS HIS INITIAL EXPERIENCE, WHICH LED TO WORKING ON COMPUTERISED ENVIRONS. ULTIMATELY WORKING IN CRYPTOGRAPHY IN EXCESS OF 15 YEARS, WHERE SECURITY IS LINE WITH OFFICIAL SECRETS ACT 1989. CERTIFIED AS ISO 9001 INTERNAL AUDITOR. AFTER LEAVING THE RAF, SMITH WORKED FOR A LOCAL COUNCIL EMPLOYED AS CORPORATE DATA PROTECTION OFFICER. HERE A NEW DICTACT OF CORPORATE INFORMATION SECURITY MANAGER, IMPLEMENTING ISO 27001 FOR THE ICT UNIT. CONTRIBUTED TO PCI DSS FOR COMPLIANCE TO REQUIREMENT 11 WITHIN CORPORATE SECURITY ROADMAP. INSTIGATED CORPORATE COMPLIANCE FOR INTER-GOVERNMENT COMMUNICATIONS. THIS ENABLER ENSURED CONTRIBUTION FOR THE PUBLIC SERVICES NETWORK (PSN), VIA GCSX AND GCF. LEAD OFFICER FOR REGIONAL ISO 27001 GOVERNANCE GROUP AND CORPORATE GOVERNANCE WORKING GROUP. CERTIFIED AS ISO 27001 LEAD AUDITOR, FEDERATION AGAINST SOFTWARE THEFT (FAST) AUDITOR. NOW CONSULTANT FOR ISO 27001, CYBER SECURITY, GOVERNANCE AND DATA PROTECTION.

NO COMMENTS YET

Speak your mind by leaving a reply

Your email address will not be published.

Name

Email

Website

Your Comment

SUBMIT COMMENT

□ NOTIFY ME OF FOLLOW-UP COMMENTS BY EMAIL.

□ NOTIFY ME OF NEW POSTS BY EMAIL.

Related readings you might like

ABOUT

MISSION (HTTP://SECURITYGLADIATORS.COM/MISSION-ABOUT-SG/)

TERMS OF USE AND DISCLOSURE (HTTP://SECURITYGLADIATORS.COM/TOS-DISCLOSURE-SG/)

PRIVACY POLICY (HTTP://SECURITYGLADIATORS.COM/PRIVACY-POLICY/)

CONTACT US (HTTP://SECURITYGLADIATORS.COM/CONTACT-US/)

WRITE FOR US (HTTP://SECURITYGLADIATORS.COM/WRITE-FOR-US-BECOME-SECURITY-GLADIATOR/)

DMCA POLICY (HTTP://SECURITYGLADIATORS.COM/DMCA-POLICY-ACTION/)

SG NEWSWIRE

GENERAL CYBER SECURITY NEWS (HTTP://SECURITYGLADIATORS.COM/INTERNET-SECURITY-NEWS/)

ORGANIZATIONS (HTTP://SECURITYGLADIATORS.COM/INTERNET-SECURITY-NEWS/ORGANIZATIONS/)

BRANDS (HTTP://SECURITYGLADIATORS.COM/INTERNET-SECURITY-NEWS/BRANDS/)

PERSONALITIES (HTTP://SECURITYGLADIATORS.COM/INTERNET-SECURITY-NEWS/PERSONALITIES/)

INFOSEC HOW TOS

GENERAL LIBRARY (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/)

AUTONOMY TOOLS (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/AUTONOMY-TOOLS/)

CYBER SECURITY (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/CYBER-SECURITY/)

PHONES AND SMART DEVICES (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/PHONES-AND-SMART-DEVICES/)

UNBLOCK WEBSITES (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/UNBLOCK-WEBSITES/)

WEB CENSORSHIP (HTTP://SECURITYGLADIATORS.COM/HOW-TO-GUIDES/WEB-CENSORSHIP/)

REVIEWS

ANTIVIRUS AND PERSONAL FIREWALL (HTTP://SECURITYGLADIATORS.COM/REVIEWS/ANTIVIRUS-PERSONAL-FIREWALL-PROGRAMS/)

VPNS AND SMART DNS (HTTP://SECURITYGLADIATORS.COM/REVIEWS/VPNS-AND-SMART-DNS/)

CLOUD BACKUPS (HTTP://SECURITYGLADIATORS.COM/REVIEWS/SECURE-CLOUD-BACKUPS/)

MALWARE AND SPYWARE PROGRAMS (HTTP://SECURITYGLADIATORS.COM/REVIEWS/MALWARE-AND-SPYWARE-PROGRAMS/)