CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

Johannesburg
23 May 2016

CYBER CRIME: RANSOMWARE LURKS DANGEROUSLY WITHIN THE INTERNET
Article by Terrance M. Booysen and peer reviewed by Craig Rosewarne (CEO: Wolfpack Information Risk (Pty) Ltd)

It was estimated by ISACA -- previously known as the Information Systems Audit and Control Association® -- that there could be as much as 5.4 billion internet-based connected devices by the year 2020. And these estimates may even exceed their original projections as technology advances with its prolific and wide-spread adoption. Similarly, Cisco IBSG also predict billions of devices within the business-to-business use of the Internet of Things (IoT) where personal computers, smart phones and home devices, tablets, electronic wearables, medical devices, clinical systems, gaming systems and similar instruments will become more vulnerable to the security risks that lurk within the internet.

But let's not forget there is a human component behind these pervasive devices; and for the sake of clarification, we distinguish two categories; namely the 'good guys' and the 'bad guys'. The so-called *good guys* include the persons who developed the software for all these convenient devices in the first place, as well as the owners of these devices who derive the intended benefits. The b*ad guys* are those who are causing all kinds of unwanted trouble; these are the fraudsters who hack into unsuspecting users' electronic devices and create all sorts of mayhem through their devious means, by unleashing malware applications which is costing the industry money running into the billions. ISACA believe that since 2012, the number of victimised enterprises -- comprising mostly small businesses -- have seen ransomware payments (to remove malware from the victim's electronic systems and devices) increasing from 2.9% to 41%*.

"Damage caused by a cyber attack today can severely impact a nation's critical infrastructure. The advent of the digital world and the inherent interconnectivity of people, devices and organisations open up a whole new playing field of vulnerabilities."

Craig Rosewarne (CEO: Wolfpack Information Risk (Pty) Ltd)

Source: Critical Information Infrastructure Protection Report 2016

Expectedly, a number of these 'intelligent' devices are armed with the owner's personal details which include their photographs, names, identity numbers, addresses and similar sensitive information. With all this in mind, these devices -- and their owners -- are all 'connected' in various ways, but especially where they are reliant upon the internet for matters such as software upgrades, virus updates, downloading applications and for forth. Then there's the attraction of social media applications such as Facebook, Twitter, LinkedIn and Mxit. Being in a digital society where many people like to share their personal information, not only is there a real danger of too much of this information falling into the wrong hands, but in many cases social media revellers are inadvertently allowing fraudsters to pin-point their physical location -- within metres of their electronically connected devices -- furthermore blissfully informing them of their routine and activities. Given these toxic circumstances, where data and location is blatantly exposed, cyber criminals have the perfect conditions to exploit millions of unsuspecting victims of these digital devices which contain vast tracts of personal and or sensitive information. Indeed, the physical safety of an individual may also be compromised as their identity and other information is 'stolen' by computer hackers with devious intentions. As the

thought of these intricately connected devices begins to settle; there may be less comfort in respect of safeguarding an individual's personal safety and information, including for that matter an organisation's commercial information and trade secrets.

In its earlier form, cyber criminals focussed mainly upon finding ways to penetrate an organisation's computer network and IT systems, and a cyber attack may initially only have been done by some geeky computer enthusiast wanting to demonstrate their computer brilliance. But as the years have passed, cyber crime has been ranked as a growing and top business risk. The use of the internet to facilitate and commit acts of cyber crime -- including industrial sabotage and espionage, terrorism, extortion and the like -- is a real occurrence and it has become a growing threat to governments, businesses and civil society. Cyber attacks are generally intended to disrupt the proper functioning of the target, but especially where the target is a critical information centre. Whilst it is extremely difficult to locate the physical location of cyber criminals -- who may operate solo or in syndicates -- they are quite particular when selecting their targets which generally include computer systems, servers or underlying infrastructure. Indeed, where there's personal information to be plundered, be this of a commercial and or of a private nature, this too will form part of their targets. Besides attacking their targets for reasons of terror, most cyber criminals have an objective of extorting money from their victims and they will embark upon any tactical means of getting the job done.

One of the methods a cyber criminal will deceive a potential victim is through the use of ransomware, which is a growing form of cyber crime on a global scale. More than 'opportunistic extortion', ransom demands have become market related and cyber criminals reportedly target and calculate their ransomware pricing on the basis of company size and value, among other factors. Once the ransomware takes hold of the victim's systems, which is unwittingly downloaded by the victim through the internet, the ransomware prevents or limits its victims from accessing their systems and data until the ransom is paid to the creator of the malware, usually via some form of online, or bitcoin payment method. In most cases, the victim's systems are usually either 'locked', thereby preventing them from using it, or their documents and files are encrypted to prevent the user from being able to have normal operations and usage of their systems. As may be expected, once the ransom is paid, there is no guarantee that the victim's data will be returned or that their system or devices will be unlocked.

"South Africa, like many developing countries, has made great strides in enhancing the security of the nation's critical infrastructures. Today's threats to cyber security require the collaboration of all: government, law enforcement and the private sector. Most importantly, members of the public have a key role to play in countering malicious threats to bolster our defence capabilities."

Peter Boxer (Deputy High Commissioner: British High Commission - South Africa)

Source: Critical Information Infrastructure Protection Report 2016

It is believed that the first form of ransomware was developed by Dr. Joseph Popp in 1989, which was called "AIDS" Trojan. In the earlier days, the transfer of the ransomware was done via the insertion of a diskette to the user's personal computer, however the damages caused in the so-called 'infancy' days of affecting personal computers with ransomware was negligible, and rarely did it alter the contents of a victim's files. Whilst the early forms of ransomware were relatively unsophisticated -- with the first attacks being reported

in 2005 -- by 2006 they became more advanced where encryption schemes were used to create massive confusion. Since then, ransomware has become increasingly malicious, effective and geographically wide spread such that with enhanced technology, ransomware can now enter a victim's system through a downloaded email file, or from a social media application, or any vulnerability in the victim's network service.

No one who makes use of the internet is immune to cyber crime, not least also contracting the risk of being affected by malware which is increasing on a daily basis, both at personal and corporate levels. Since ransomware attempts to intimidate victims into handing over money, it is viewed as extortion, which is a criminal offence in South Africa, governed mainly by the Electronic Communications and Transactions Act 25 of 2002 and the Cybercrimes and Cybersecurity Bill 2015. Other South African legislation with bearing on cyber crime includes the Protection of Personal Information Act 2013 (POPI), the Regulation of Interception of Communications & Provision of Communication-related Information Act 2002 (RICA), the Criminal Procedure Act 1977 and the Prevention and Combatting of Corrupt Activities Act 2004 (PRECCA).

On the international front, new cyber security rules were agreed in December 2015 by lawmakers in the European Union ('EU'), after nearly two years of negotiations. The draft Network and Information Security ('NIS') Directive is still to be formally approved by the EU Parliament's Internal Market Committee and the Council Committee of Permanent Representatives. EU countries will have 21 months in which to transform the NIS Directive into national laws and then a further six months to identify the operators of essential services that will be subject to the rules in their jurisdiction. The NIS Directive will require organisations to put appropriate security measures in place to protect their networks and data against cyber security incidents and they will be compelled to report serious breaches to the appropriate regulators. Similarly in the United States of America, US Congress passed the Cybersecurity Act of 2015 in order to defend victims against cyber attacks. Interestingly, the US' Cybersecurity Act aims to provide its government entities and the private-sector a common framework to encourage voluntary sharing of cyber security threat information, which must be done in a responsible manner.

There's no doubt that cyber crime and ransomware are here to stay; and if the internet is to survive and grow further to improve the manner in which human beings wish to stay connected, and learn yet more about each other, we will need to urgently address the issue of trust and security over the internet. The more people and organisations that are left exposed to faceless cyber criminals, the less the internet will be trusted and used. This in turn could cause our modern and highly connected world to revert back to a bygone era when trusted communication was available only to a select group of individuals.

*Source: ISACA Identifies Five Cyber Risk Trends for 2016

ENDS
Words: 1,705

CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

Further Contact Information:

Terrance M. Booysen (CEO)
CGF Research Institute (Pty) Ltd
Office: (011) 476 82 64 / 1 / 0 Cell: 082 373 2249
Email: tbooysen@cgf.co.za
Twitter : @CGFResearch

Craig Rosewarne (CEO)
Wolfpack Information Risk (Pty) Ltd
Office: (011) 794 7322
E-mail: craig@wolfpack.com
Web: www.wolfpackrisk.com

About CGF Research Institute (Pty) Ltd: Services

CGF is a Proudly South African, Level 4 B-BBEE compliant company that specialises in conducting desktop research on Governance, Risk and Compliance (GRC) topics, amongst other related company secretariat, regulatory and compliance consulting services.

The company has developed numerous products that cover GRC reports designed to create a high-level awareness and understanding of issues impacting a CEO through to all employees of the organisation.

Through CGF's Lead Independent Consultants, our consulting capabilities include the aggregation of local and international best of breed governance reporting services and extend to;

– strategic management consulting, business re-structuring, executive placements, executive coaching, board assessments and evaluation, out-sourced company secretrial functions, facilitation of Corporate Governance Awareness workshops, IT governance through to Enterprise Risk Management (ERM) consulting and Corporate Reputation services. All CGF's services cater for large corporates, small and medium sized businesses and state owned organisations.

To find out more about CGF, its Lead Independent Consultants and Patrons access *www.cgf.co.za* or *www.corporate-governance.co.za*