Media Contact:

Teresa Settas

Teresa Settas Communications

+27 11 894 2767

teresa@tscommunications.co.za

**Cyber risks Severely Underrated by EMEA Businesses**

*SA is 5th most targeted country in the world cybercrime*

[Feb 2015]: South Africa is the 5th most targeted country in the world in terms of cybercrime attacks, while informal consensus within the private sector places SA third behind Russia and China. Cybercrime is any crime involving a computer or internet and SA is perceived by syndicates as fertile ground for hacking attacks as they believe there is little chance of arrest and successful conviction on SA soil. Beyond the immediate threat of cyberattacks, the criminal activity is also linked to other illegal activities such as human trafficking, drug smuggling and money laundering.

“Despite the potentially devastating financial, legal and reputational consequences of a major cyber breach on a corporate entity, there is widespread apathy across SA’s business sector to insure their bottom lines against serious losses and the cost of recovery due to cybercrime attacks. Another challenge is that most attacks are underreported, as no business wants to admit publicly that they have been compromised, despite them being legally compelled to inform all clients of any breach that could compromise their personal data,” explains Kerry Curtin, Principal Broker: Financial Institutions & Professional Risks at [Aon South Africa](https://www.aon.co.za),

A report by Aon, a global risk advisory and insurance brokerage titled ‘[Exploring the Latest Cyber Risk Trends in EMEA](http://www.aon.com/forms/form-2012-ars-fsg-cyber.html)’ shows that there is still a low level of Board involvement in actively addressing cyber risk management across the EMEA. Not surprisingly, this is also reflected in the Global Average. These findings are alarming when one considers that the report shows that in some EMEA countries a large percentage of companies had a data breach or a serious technical outage in a defined 12 month period, while the global average indicates that one in three companies report suffering from some type of incident during the same period.

“Based on local take up of specialist cyber risk insurance, we estimate that over 70% of South African businesses, including large corporates and institutions are woefully unprepared for the financial, legal and reputational ramifications of a major cyber hack. Recent news headlines provide compelling reason for business leaders to get very serious about managing their cyber risks and it should be a priority in boardrooms, law enforcement agencies and intelligence units. There will be increasing pressure on an organisation’s Board to familiarise themselves with the company mechanisms associated with cyber risk and security. Recent high profile cyber-attacks and subsequent losses have left the positions of high profile executives untenable. An understanding of the severity of the threat has become an absolute requirement, imperative to the future of the business in many cases. Cybercrime is alive and well on South African soil and costs the economy an estimated R6 billion a year, a figure that’s steadily growing,” says Kerry.

In May 2014, an international cybercrime syndicate was exposed with 12 people arrested on South African soil in Pretoria, while another 10 were arrested in the United States and Canada. The arrests came after a joint operation between the Hawks, Crime Intelligence, SA Tactical Response Team and department of home affairs and Interpol, the US Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI).

In Washington last year, hackers took over Twitter accounts of the *New York Post* and United Press International, writing messages including about hostilities breaking out between the United States and China. Several media organisations have also had their Twitter feeds hacked over the past two years including AFP and the BBC, and locally the Star newspaper.

But by far, the most unprecedented hack ever inflicted on a business was on Sony Pictures in December 2014. The hack even escalated to threats of terrorism, forcing Sony to cancel the release of its movie ‘The Interview’. Sony’s reputation is in tatters as a result of revelations from highly sensitive information being released in the public domain, and is possibly the costliest ever for a US company.

“South African businesses are in no way insulated from suffering such a catastrophic breach and cyber-crime is already having a significant economic impact on the country, and is expected to get worse. According to a report compiled by McAfee software on behalf of the Center for Strategic and International Studies (CSIS), the ‘[Global Cost of Cyber-crime’](http://csis.org/event/2014-mcafee-report-global-cost-cybercrime) report puts the cost of cyber-crime to the global economy in the region of US$400 billion. In South Africa, the McAfee report says that the economic impact of cybercrime locally is equal to about 0.14% of the country’s total GDP. With a GDP contribution of R4.1trillion, that means that cybercrime is costing SA almost R6 billion per year,” she says. And while lower-income countries may have smaller losses now, this will change as these countries increase their use of the Internet and as cybercriminals move to exploit mobile platforms.

“But by far, the greatest cost to companies is the clean-up afterwards. While criminals may not be able to monetise all their gains from an attack, victim companies still have to put measures in place as if they have lost all their data to criminal threats. The aggregate cost for recovery is far greater than the gains by cybercriminals,” says Kerry.

The very nature of the internet means that cyber criminals from anywhere in the world can direct their attention to specific targets. It’s also believed that local hackers could be more organised than previously thought, as per the recent rise of hacker group Anonymous with its South African chapter.

“Amidst all the cyber mayhem, South African businesses are still slow to understand that Network Security and Privacy risks are emerging and constantly evolving issues, and businesses must ensure that adequate measures are in place to address them, including systems and processes on the IT front in relation to harvesting, storing and disseminating information, and controls around personnel access,” she warns.

In this regard, Aon’s recently launched [Cyber Diagnostic Tool](https://www.aoncyberdiagnostic.com/) aims to help risk managers better identify and understand their exposure to cyber risk. The tool uses a series of multiple choice questions to assess how employees use technology, the current controls in place and management’s attitude to cyber risk. The tool then provides meaningful insight into the most important cyber risk topics and includes practical guidance on related governance frameworks that should be in place, as part of an effective cyber risk management strategy.

Local companies could soon also be forced to comply with US Security and Exchange Commission requirements too. It is mandatory for companies situated in the United States to notify an entire database of a security breach, which can be very costly. This could very soon become mandatory for South African businesses who encounter a cyberattack. This in turn is expected to drive demand for insurance products to protect businesses exposed to a virus or hacking attacks as cyber and IT risks become more aggressive, and very public knowledge.

**Cyber risk demands specialist insurance cover**While liability policies generally only respond to third party claims, certain cyber liability policies will also provide first party cover – in other words cover for the costs incurred by the policy holder to rectify and recover from the breach.

According to Aon, only specialist cyber insurance policies provide extensive cover, and cover expenses such as immediate crisis management, forensic analysis, the reparation of computer systems and any loss of income resulting from a cyber attack. Standard policies are often inadequate to cover the likely cost of even a more “standard” security breach, let alone cyber-attack or ‘hacktivism’. Third party costs such as customer compensation and any legal expenses can also be covered by cyber insurance and potentially save companies millions should they be subject to a breach or attack.

Aon identified some gaps in cover under current conventional insurances that could be leaving businesses vulnerable to being liable in the event of a Network Security and Privacy (NSP) incident:

* General liability, material damage and property policies are designed to respond to natural disasters that damage physical assets. The loss does not extend to intangible assets, nor does it extend to losses caused by non-physical perils such as viruses or hackers.
* Professional indemnity policies cover damage resulting from a failure of the defined professional services, and may not extend to losses resulting from data and privacy breaches.
* Crime policies generally cover only money, securities and tangible property with no coverage for third party property such as customer data. Computer fraud coverage may not exist for third party losses due to computer viruses or unauthorised access to confidential information.
* Many insurance policies also have defined geographical coverage limitations.

As NSP risk advances as an issue and the regulatory landscape continues to adjust, businesses need to check their current insurance cover and ensure they are not vulnerable to significant damages should they fall victim to cybercrime.

“Companies need to consider the security implications that their businesses are exposed to. Over and above investigating insurance options, local businesses should ensure that firewalls, IT security and virus protection measures are properly in place and regular tests are run to gauge effectiveness. Regardless of size or status, no business is safe from e-threats, unless it includes security as its ultimate priority. There is no one size fits all approach to cyber insurance. It all depends on the size of the company, nature of its business and its unique levels of exposure. In this regard, consulting with a professional risk advisor is an invaluable exercise in protecting your reputation, data, clients and income,” concludes Kerry.

Ends…

**About Aon South Africa**

Aon  South  Africa  is  a  leading  provider  of  risk management services, insurance   and   reinsurance   brokerage,  human  capital  and  management consulting, and speciality insurance underwriting. The company employs more than 1300 professionals in its 16 offices in South Africa with its head office in Sandton Johannesburg. Aon employs over 1800 people on the African continent.

Facebook - <https://www.facebook.com/AonSouthAfrica>

Twitter - <https://twitter.com/Aon_SouthAfrica>

LinkedIn - <http://www.linkedin.com/company/aon-south-africa>

Sign up for News Alerts: <http://aon.mediaroom.com/index.php?s=58>

**About Aon**

[Aon plc](http://www.aon.com) (NYSE:AON) is the leading global provider of [risk management](http://www.aon.com/risk-services/default.jsp), insurance and [reinsurance](http://www.aon.com/reinsurance/default.jsp) brokerage, and [human resources](http://www.aon.com/human-capital-consulting/default.jsp) solutions and [outsourcing](http://www.aon.com/human-capital-consulting/hrbpo/default.jsp) services. Through its more than 66,000 colleagues worldwide, [Aon](http://aon.mediaroom.com/) unites to empower results for clients in over 120 countries via [innovative](http://www.insurancejournal.com/news/international/2012/12/12/273624.htm) and effective [risk](http://www.aon-esolutions.com/) and [people](http://www.aon.com/human-capital-consulting/default.jsp) solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world’s best [broker](http://aon.mediaroom.com/2013-02-21-Risk-Insurance-magazine-honors-47-Aon-brokers-and-consultants-with-Power-Broker-designation), best insurance intermediary, best reinsurance intermediary, best captives manager, and best [employee benefits](http://www.aon.com/human-capital-consulting/consulting/health_benefits_consultants.jsp) consulting firm by multiple industry sources. Visit [aon.com](http://aon.com) for more information on Aon and [aon.com/manchesterunited](http://www.aon.com/manchesterunited) to learn about Aon’s global partnership with [Manchester United](http://www.manutd.com/Splash-Page.aspx).