Cyber Crime Proposal Form

Private and Confidential

Cyber crime is not a fictional concept: it is a very real problem. Last year the cost of global cyber crime was estimated to be USD388bn-with an individual falling victim to a form of online crime every 19 seconds.
In today’s multi-channel, mobile and interconnected world, every element of society including government, industry, commerce, charity, health, education and individual citizens is increasingly at risk as more and more sensitive data is stored on a computer system somewhere in the world .the risks are constantly evolving as technology develops ,and they are likely to become more acute as a new generation of smartphones effectively become mobile wallets, which will place ever greater volumes of personal and financial data at a risk.
Our goals were to:

- Define cyber threats to domestic and global businesses
- Quantify the costs of a data breach
- Understand current and future legal requirements

Threat is growing
Criminals looking to steal and exploit data for financial gain are in an increasingly strong position. Not only does new technology and growing access to that technology provide even more opportunity, but government and private enterprises are aware that they can no longer keep quiet about data leaks and malicious attacks on their IT systems. While it is good to keep the public informed, any release of information on the nature and extent of cyber attacks and how to prevent them also educates the fraudsters and raises the threat level further.
Regulatory change is happening
Regulators across the world are waking up to the fact that changes in data privacy laws are required.
Cost of data breaching is rising
One certainty in this complex and fast moving area breaches are becoming more common and dealing with them increasingly costly, complex and damaging for the organization that owns’ the data.Nortons Cybercrime Report for 2011 estimates that the cost of stolen cash and cost of time spent on identifying and resolving data breaches to businesses and governments is around USD 358bn globally
Three key causes of loss

- Hackers and criminals were responsible for 32% of breach events
- Rogue employees were the cause of 19% of data breaches –and the poor economic climate is expected to exacerbate this problem going forward.

Theft of mobile computer equipment such as laptops and memory sticks carrying unencrypted data was responsible for 33% of breaches

WHAT ARE THE MAIN CYBER RISKS?
The connectivity that technology creates brings many business benefits, but there is a flip side. With the proliferation of mobile devices including blackberries, iPhones, smartphones, notebooks and iPads, commercial organizations are opening themselves up to new and growing threats from the risk of cybercrime and data loss

Full name of Proposer(s): ____ PIN No: __________________

Postal Address: ______________________ Postal Code: _____________________Town: ____________________

Telephone No. - Office: _______________________Mobile Phone: ____________________ Fax No.: ___________

Email Address: _______________________________________Website:__________________________________

Business or Profession: ____

Name of Contact Person: ____Position: ____________________

Physical Address: Bldg: _______________________ Floor: ____________Street: __________________________

Period of Insurance: From_______________________ To_______________________________________

Desired Coverages

Covers required

- ☐ Network Security and Privacy Liability
- ☐ Multimedia Liability
- ☐ Privacy Regulatory Defence and Penalties
- ☐ Business Interruption and Additional Costs of Working
- ☐ Crisis Management
- ☐ Cyber Extortion

Financial information

Gross Annual Revenue

Last Year	Kshs.
Current Year	Kshs.
Next Year (estimated)	Kshs.

% of gross annual revenue account for by sales or operations through your website ______ %

% of annual transactions paid by debit/credit card	%
Average Transaction value	Kshs.
Percentage of last year's gross annual revenue generated from:	%
	%
	%
IT system budget	Kshs

Network and Data Security

Do you store, process and or transmit any Sensitive Data on Your Computer System *(Tick all that apply)*

- ☐ Credit card information
- ☐ Customer Information
- ☐ Healthcare information
- ☐ Money/Securities information
- ☐ Trade Secrets
- ☐ Intellectual Property Assets

Do you process payments on behalf of others, including e-Commerce transactions? ☐ Yes ☐ No

Do you outsource any part of Your network, computer system or information security functions? Tick all that apply

		Vendor name providing services
Data center hosting	☐	
Managed Security	☐	
Data Processing	☐	
Application service Provider	☐	
Alert log monitoring	☐	
Offsite backup and storage	☐	

Do you require all vendors to whom You outsource data processing or hosting functions (e.g. data backup, application service providers etc) to demonstrate adequacy of their IT systems? ☐ Yes ☐ No

If 'Yes', please indicate method of verification

Do you have strict user revocation procedures on user accounts and inventoried recovery of all information assets following employee termination? ☐ Yes ☐ No

Do you have anti-virus software on all computer devices, servers and networks that are updated in accordance with the software providers' recommendations? ☐ Yes ☐ No