Cyber Security vs Cyber War: What everyone should know

28 November 2018
Durban, KZN

Presented by Sadé Savings of UpperHand Cyber Security Solutions
Defining key concepts
Current cost to African economy
Risks and threats
Technology trends in 2018
The Big Opportunity everyone should know about (and act on)
What is Cyber Security

Cyber Security refers to:
“the policies, procedures and processes performed by an organization to ensure that information relevant to them that is stored in cyber space is preserved regarding their confidentiality, integrity, and availability.”

https://www.bcmpedia.org/wiki/Cyber_Security
What is Cyber War/

Cyber war:
- The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.
- “… is asymmetric, which means it benefits lesser military powers as much as military goliaths.”

https://en.oxforddictionaries.com/definition/cyberwar
The Cost to Africa

- Estimates are at $3.5 billion in 2017
- 90% of African businesses are not equipped to effectively protect themselves
Cybercrime threats remains pervasive across Africa

<table>
<thead>
<tr>
<th>Threat</th>
<th>Cost (2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider threat</td>
<td>$352 million</td>
</tr>
<tr>
<td>Attack on computer systems</td>
<td>295</td>
</tr>
<tr>
<td>Identity theft</td>
<td>166</td>
</tr>
<tr>
<td>Email spam</td>
<td>108</td>
</tr>
<tr>
<td>Data exfiltration</td>
<td>75</td>
</tr>
<tr>
<td>Online fraud scams</td>
<td>82</td>
</tr>
</tbody>
</table>
Africa's banking sector faces the highest risk from cybercrime

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost (2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; financial services</td>
<td>$248 million</td>
</tr>
<tr>
<td>Government</td>
<td>204</td>
</tr>
<tr>
<td>E-commerce</td>
<td>173</td>
</tr>
<tr>
<td>Mobile/e-payments</td>
<td>140</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>119</td>
</tr>
</tbody>
</table>
1. Ransomware: Ransomware attacks have been projected to increase in volume and sophistication.

2. Business E-mail Compromise (BEC): BEC attacks are forecast to cost in excess of $9 billion (globally) in 2018.
3. Crypto Currency or Coin Mining: the rise of crypto currency has resulted in an 8500% increase in coin mining as cyber criminals ‘steal computer processing power to mine crypto currency’.

4. Mobile Malware: attacks on mobile devices have increased drastically, and even Macs and devices running on iOS that were previously thought to be “safe and virus free” have seen a 500% surge in ransomware attacks.
5. Mobile Banking Malware: presents a massive risk, particularly for the African market where mobile Fintech solutions are a key driver of innovation for largely unbanked populations.

6. Internet of Things (IoT): as the number of connected “things” continues to grow; securing IoT devices presents a major challenge that could potentially lead to security breaches that are more widespread and complex than we have seen to date.
The biggest Cyber threat is not technological.

64% of Cyber Security incidents are attributed to users and employees inside an organization (Insider Threat Report 2018).
Technology & Innovation Trends in 2018

Trend 1: Zero-Trust Security Model
Only users that have been verified through rigorous and multi-layered authentication measures will gain access to systems.

Trend 2: Deception Technologies
Deception Technologies will allow organisations to detect cyber risks faster and track their point of origin.
Trend 3: Behavioural Analytics and Artificial Intelligence

A technique known as ‘deep learning’ will enable machines and intelligent devices to predict whether the person accessing the system is a ‘safe user’.

Trend 4: Automated threat seekers

Enabled by Artificial Intelligence will ‘hunt’ potential risk and threat and isolate it before it can potentially become perilous.
Trend 5: Blockchain

Acting as a digital ledger, Blockchain technology has potential to give organisations more control over information and highlight any suspicious behaviour.
The Cyber Opportunity everyone should know about (/>

- 3.5 million unfilled Cyber Security positions (CyberSecurity Ventures)

- Zero per cent unemployment rate

Africa’s challenge: High levels of (youth) unemployment across the continent are prohibiting the continent’s progress towards achieving the Sustainable Development Goals (SDG’s).
The Cyber Opportunity everyone should know about

The gap in the Cyber Security market for trained and skilled individuals presents all interested stakeholders with an opportunity to develop a long-term, sustainable solution to two of Africa’s biggest challenges.

1. Increasing cyber threat
2. High unemployment levels
<So What? />

- A concerted effort to move from an *awareness* of Cyber Threat to the active and strategic *implementation* of policies and frameworks is critical.

- A commitment to innovation in preventing and predicting future Cyber Threat is imperative for all stakeholders concerned with realising Africa’s full potential.
<So What? />

Investing in skills and individuals to pursue careers in the field of Cyber Security is in fact the key opportunity that everyone should be aware of and act on.
First ever online cyber security training academy built for Africans, by Africans.
<Thank You

Ngiyabonga

Merci Beaucoup

Obrigado

Dankie />

Sadé Savings
+27 82 852 1653
sade@upperhandcyber.com