Cybercrime – Security Risks and Challenges Facing Business

Sven Hansen
Technical Manager – South Africa
Agenda

1. What is Cyber Crime?
2. Cyber Crime Trends
3. Impact to Business
4. Managing the Risk
5. Path to Cyber Resilience
Before jumping in – what is Cybercrime exactly?

• The simple answer is...

**It's complicated!**

Council of Europe - Cybercrime Treaty defines it as: data used for criminal purposes, all the way to copyright infringement

While United Nations include Fraud, Forgery and unauthorized access as Cybercrimes.

**Symantec** – *Any crime using a computer, hardware device or network – where the computer is an agent, facilitator or target of the crime.*
Cyber Threat Landscape – some statistics

250,000 web attacks blocked daily by Symantec in 2012

1 in 532 websites were infected

1.6 million new malware variants discovered daily
Symantec Global Intelligence Network

Identifies more threats, takes action faster & prevents impact

Worldwide Coverage

Global Scope and Scale

24x7 Event Logging

Rapid Detection

Attack Activity
- 240,000 sensors
- 200+ countries

Malware Intelligence
- 133M client, server, gateways monitored
- Global coverage

Vulnerabilities
- 40,000+ vulnerabilities
- 14,000 vendors
- 105,000 technologies

Spam/Phishing
- 5M decoy accounts
- 8B+ email messages/day
- 1B+ web requests/day

Preemptive Security Alerts

Information Protection

Threat Triggered Actions

East Africa Security Conference – August 2013
Agenda

1. What is Cyber Crime?
2. Cyber Crime Trends
3. Impact to Business
4. Managing the Risk
5. Path to Cyber Resilience
Symantec Internet Security Threat Report Findings 2012

Targeted Attacks up 42% in 2012

Social Media
Tailored & Specific

Mobile Malware
58% increase

State Sponsored Attacks Increased Dramatically
Manufacturing moved to top position in 2012

But all industries are targeted

DID YOU KNOW?

Every organization is a potential target
Targeted Attacks by Company Size

- Greatest growth in 2012 is at companies with <250 employees

50% 2,501+

50% 1 to 2,500

- 1 to 250
  - 31%
  - 18% in 2011

- 501 to 1,000
  - 5%
  - 3%

- 1,001 to 1,500
  - 3%

- 1,501 to 2,501
  - 9%

- 2,501+
  - 50%

East Africa Security Conference – August 2013
## Africa specific data

Taken from Symantec Internet Security Threat Report 18

### Top Ten Overall

<table>
<thead>
<tr>
<th>#</th>
<th>Country</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>South Africa</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Morocco</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Tunisia</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Algeria</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Mauritius</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Nigeria</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>Kenya</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Sudan</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>Ghana</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>Cameroon</td>
<td>10</td>
</tr>
</tbody>
</table>

### Top Ten Phishing

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>South Africa</td>
<td>40.1%</td>
</tr>
<tr>
<td>2</td>
<td>Morocco</td>
<td>31.7%</td>
</tr>
<tr>
<td>3</td>
<td>Mauritius</td>
<td>9.5%</td>
</tr>
<tr>
<td>4</td>
<td>Seychelles</td>
<td>6.7%</td>
</tr>
<tr>
<td>5</td>
<td>Kenya</td>
<td>2.7%</td>
</tr>
<tr>
<td>6</td>
<td>Tunisia</td>
<td>1.2%</td>
</tr>
<tr>
<td>7</td>
<td>Zambia</td>
<td>1.2%</td>
</tr>
<tr>
<td>8</td>
<td>Botswana</td>
<td>0.9%</td>
</tr>
<tr>
<td>9</td>
<td>Angola</td>
<td>0.9%</td>
</tr>
<tr>
<td>10</td>
<td>Libya</td>
<td>0.8%</td>
</tr>
</tbody>
</table>
Africa specific data

Taken from Symantec Internet Security Threat Report 18

Top Ten Spam

1. Morocco - 26.2%
2. Tunisia - 19.4%
3. South Africa - 9.4%
4. Mauritius - 8.4%
5. Sudan - 6.6%
6. Algeria - 4.0%
7. Nigeria - 3.3%
8. Senegal - 3.1%
9. Libya - 2.7%
10. Ivory Coast - 2.6%

Top Ten Virus

1. South Africa - 19.0%
2. Algeria - 10.1%
3. Nigeria - 8.8%
4. Morocco - 6.5%
5. Tunisia - 4.0%
6. Mauritius - 3.7%
7. Ghana - 3.3%
8. Ethiopia - 3.3%
9. Cameroon - 3.0%
10. Kenya - 3.0%
What Drives the Modern Day Attacks?

Hacktivism
- DDoS
- Defacement

Targeted Attacks
- Sabotage
- Espionage

Money
- Banking Trojan
- Extortion
- Scam
What this means to business

- Technology and business are indelibly linked.
- But it is a double edged sword

New customers are online, mobile and connected.

- There is no silver bullet – eliminating risk is impossible and it impedes agility.

  - **Organizations need to define their risk appetite**
  - **Goal is to become Cyber Resilient**
So what is Cyber Resilience?

• Some existing definitions:

1. **Resilience** is defined as the ability of an ecosystem to return to its original state after being disturbed. *(Wikipedia)*

2. **Cyber-resilience** is the organization's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace. *(Information Security Forum)*

3. **Cyber-resilience** is defined as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery. *(World Economic Forum)*
## Cyber-Resilience Framework

<table>
<thead>
<tr>
<th>KNOW</th>
<th>HUMAN</th>
<th>TECHNOLOGY</th>
<th>PROCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Research Study</td>
<td>Find/Capture</td>
<td>Collect</td>
</tr>
<tr>
<td></td>
<td>Publish</td>
<td>Categorize/store</td>
<td>Analyse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aggregate/Correlate</td>
<td>Map</td>
</tr>
<tr>
<td>PREVENT</td>
<td>Recruit Educate</td>
<td>Define</td>
<td>Evaluate vital assets</td>
</tr>
<tr>
<td></td>
<td>Train</td>
<td>Build</td>
<td>Analyse risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintain</td>
<td>Define policies</td>
</tr>
<tr>
<td>DETECT</td>
<td>Search Identify</td>
<td>Monitor</td>
<td>Guide</td>
</tr>
<tr>
<td></td>
<td>Notify</td>
<td>Analyse</td>
<td>Inform</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alert</td>
<td>Decide</td>
</tr>
<tr>
<td>RESPOND</td>
<td>Apply Render</td>
<td>Block</td>
<td>Communicate</td>
</tr>
<tr>
<td></td>
<td>Justify</td>
<td>Remediate</td>
<td>Follow-up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Restore</td>
<td>Evaluate impacts</td>
</tr>
<tr>
<td>CONTROL</td>
<td>Evaluations</td>
<td>Audits</td>
<td>Compliance</td>
</tr>
</tbody>
</table>
Agenda

1. What is Cyber Crime?
2. Cyber Crime Trends
3. Impact to Business
4. Managing the Risk
5. Path to Cyber Resilience
A Taxonomy of Risk

Enterprise Risk

Reputational Risk

Strategic Risk

Financial Risk

Market Risk

Credit Risk

Operational Risk

Other Operational Risks

IT Risk

Security Risk

Compliance Risk

Availability Risk

Performance Risk

East Africa Security Conference – August 2013
Define Risk Appetite

Likely Impact

Very High
High
Medium
Low

Un-acceptable Risk

Acceptable Risk

Likelihood of event

Very Low
Low
Medium
High
Very High

East Africa Security Conference – August 2013
Quantifying Risk Appetite

<table>
<thead>
<tr>
<th>Likely Impact</th>
<th>Very High</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>X - Risk 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Flood)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td>X - Risk 2</td>
<td>X - Risk 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Server Failure)</td>
<td>(DoS Attack)</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X - Risk 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Malware Outbreak)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Likelihood of event

East Africa Security Conference – August 2013
Additional Considerations

- Business and IT need to identify risks together
  - Working in isolation creates disconnect
  - Do all parties agree on what is critical?

- Clearly define who is responsible for specific risk
  - Network Team
  - Security Engineers
  - IT Operations

- Consistently measure and feedback on changing risk posture
1. What is Cyber Crime?
2. Cyber Crime Trends
3. Impact to Business
4. Managing the Risk
5. Path to Cyber Resilience
Path to Cyber Resilience

1) Don’t think too small

• Not many organizations can afford dedicated security team

• Bad guys are organized and smart

• Security Basics revisited – do we need MORE tools?

Collaboration Across EAC

• Organizations and security teams need to work together
• Share knowledge / Pool resources
Path to Cyber Resilience

2) Fighting yesterday’s battle

• *Multiple attack vectors – subtle, distributed and personalized*

• *Single ‘Wall of Steel’ will fail – ‘Defense in Depth’ approach is required.*

• *Crucial to have relevant and timely data about your ICT infrastructure.*

So what do the new attacks look like?
Social Media & Phishing Examples

You have new notifications.
A lot has happened on Facebook since you last logged in. Here are some notifications you've received from Technical Support.

Your profile has been successfully updated.

View Notifications  Go to Facebook

This message was sent to swanhansens@hotmail.com. If you don’t want to receive these emails from Facebook in the future, please unsubscribe.

Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

“hello have you seen this recent video on the president? What is he doing in it? Omg.. LOL http://goo.gl/z1XRR...” th hi ka hriat miah lovin ka lo sent vak mai a, a ngaihna ka se lo, lo hmu khain gaidam teh u...piz...

hzjqorbmdnf – Powered by CO.CC
www.hzjqorbmdnf.co.cc

about an hour ago
The Hackers View

Organized & Professional
# The Hackers View

**Organized & Professional**

![CrimePack Interface Screenshot](image)

## Overall Stats

<table>
<thead>
<tr>
<th>unique hits</th>
<th>loads</th>
<th>exploit rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

## Exploit Stats

<table>
<thead>
<tr>
<th>iepeers</th>
<th>msiemc</th>
<th>pdf</th>
<th>mdac</th>
<th>hcp</th>
<th>java</th>
<th>webstart</th>
<th>java-getval</th>
<th>activex</th>
<th>other</th>
<th>aggressive</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## OS Stats

<table>
<thead>
<tr>
<th>os</th>
<th>hits</th>
<th>loads</th>
<th>rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>windows 2k</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>windows 2k3</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>windows xp</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>windows vista</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

## Browser Stats

<table>
<thead>
<tr>
<th></th>
<th>(0 loads)</th>
<th>0%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Path to Cyber Resilience

3) Include all employee’s

• Employee’s are companies greatest asset – and also biggest security risk

• Security is everyone’s responsibility – not only IT.

  \textbf{Is your supply chain secure?}

• Security Awareness Campaigns

  Help employee’s understand impact of \textit{Shadow IT}, and \textit{BYOD}.
Path to Cyber Resilience

4) Understand your organization profile

- Now that the risk appetite is identified – measure continuously and seek **IMPROVEMENT**

- Base-lining and auditing

- Standards and regulatory compliance

- Incident Response
Path to Cyber Resilience

5) Make Cyber resilience your competitive advantage!

- 60% of companies that lost their data – shut down in 6 months
- 93% of companies that lost DC services for 10 days – were bankrupt in one year

Recent survey shows 54% of SMB’s don’t do daily backups!
Call to Action!

1. Establish your risk profile and know your exposure
2. Make **people** part of Cyber Resilience
   - Educate the employee’s
   - Educate the supply chain & all stakeholders
3. Use Cyber Resilience as long term strategic competitive advantage.
4. Reference existing frameworks / Engage **Security** vendors
Thank you!

Sven Hansen
Sven_Hansen@symantec.com
@Sven_Hansen_Sym