

Rise of Cybercrime

Getting to grips with today's
growing cyber-threats

June 2016

The global cyber threat landscape has shifted radically

New threat actors have emerged in recent years, including nation states, organised criminals, insiders, hacktivists and cyber terrorists

Their **motivations are varied**, with some purely interested in financial gain while others may be driven by the advancement of a political agenda

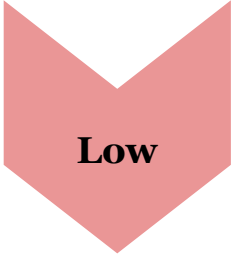




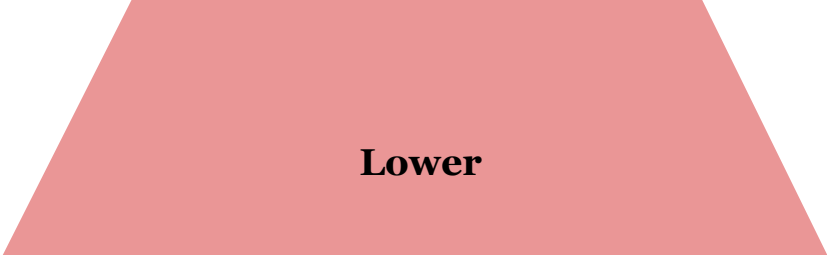
Malware and attacks are increasingly sophisticated. Commercial exploit kits and source code are widely available, reducing the time to create new malware and enabling more innovative attacks.

Cybercrime is growing

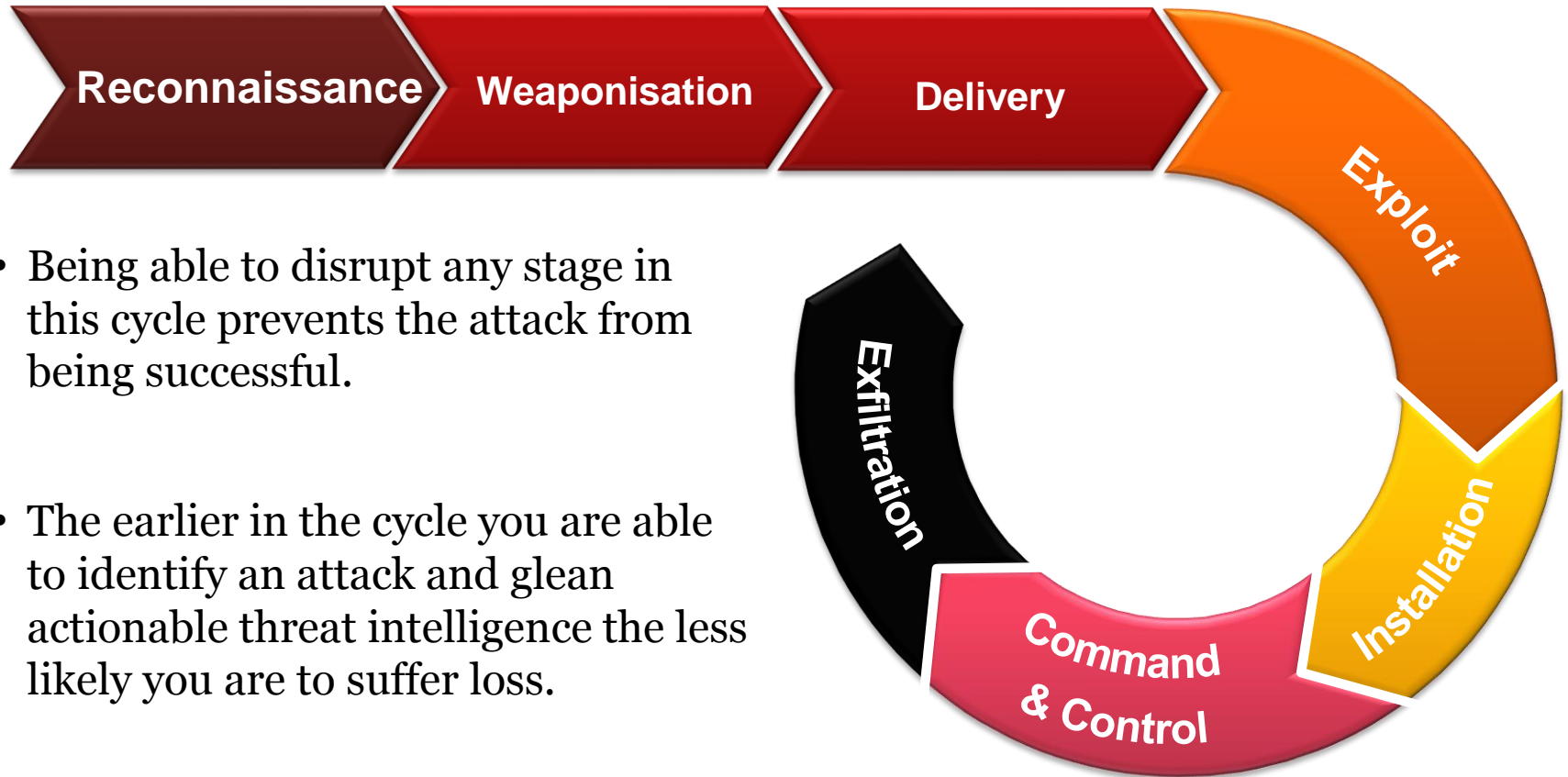
- Cybercrime incidents **continue to rise** and the **threat landscape** is fundamentally changing.
- Many organisations seem only to take notice of cyber security **after an attack**, believing that only **big US Companies** are under serious attack
- Traditional organisational structures tend to be too **slow and rigid** to enable the speed and flexibility of response needed in the cyber world
- Cybercrime produces **high returns at low risk** and relatively low cost for the Hackers



Cyber attacks have a very low barrier to entry

<i>Probability</i>	<i>Example</i>	<i>Impact</i>
 Low	Insider attack Theft of IP APT's Industry specific attacks	 High
 Medium	IT network breach System infiltration Industry targeting	 Medium
 High	Traditional attacks Untargeted phishing Malicious links Denial of service	 Lower

The intrusion chain to gain access



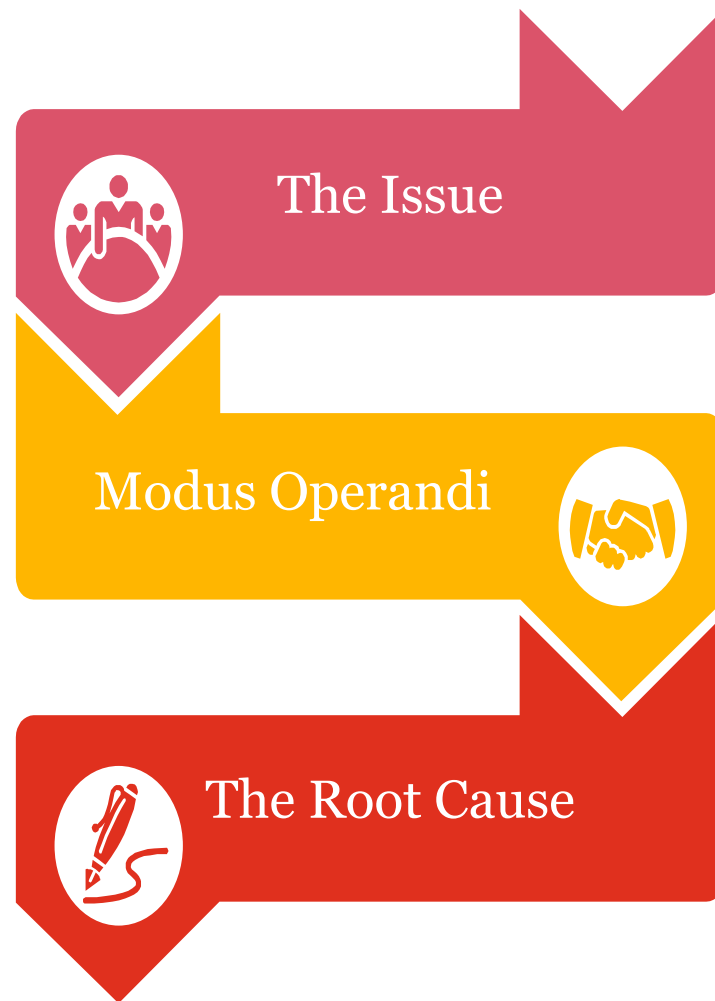
- Being able to disrupt any stage in this cycle prevents the attack from being successful.
- The earlier in the cycle you are able to identify an attack and glean actionable threat intelligence the less likely you are to suffer loss.

Case in point.....

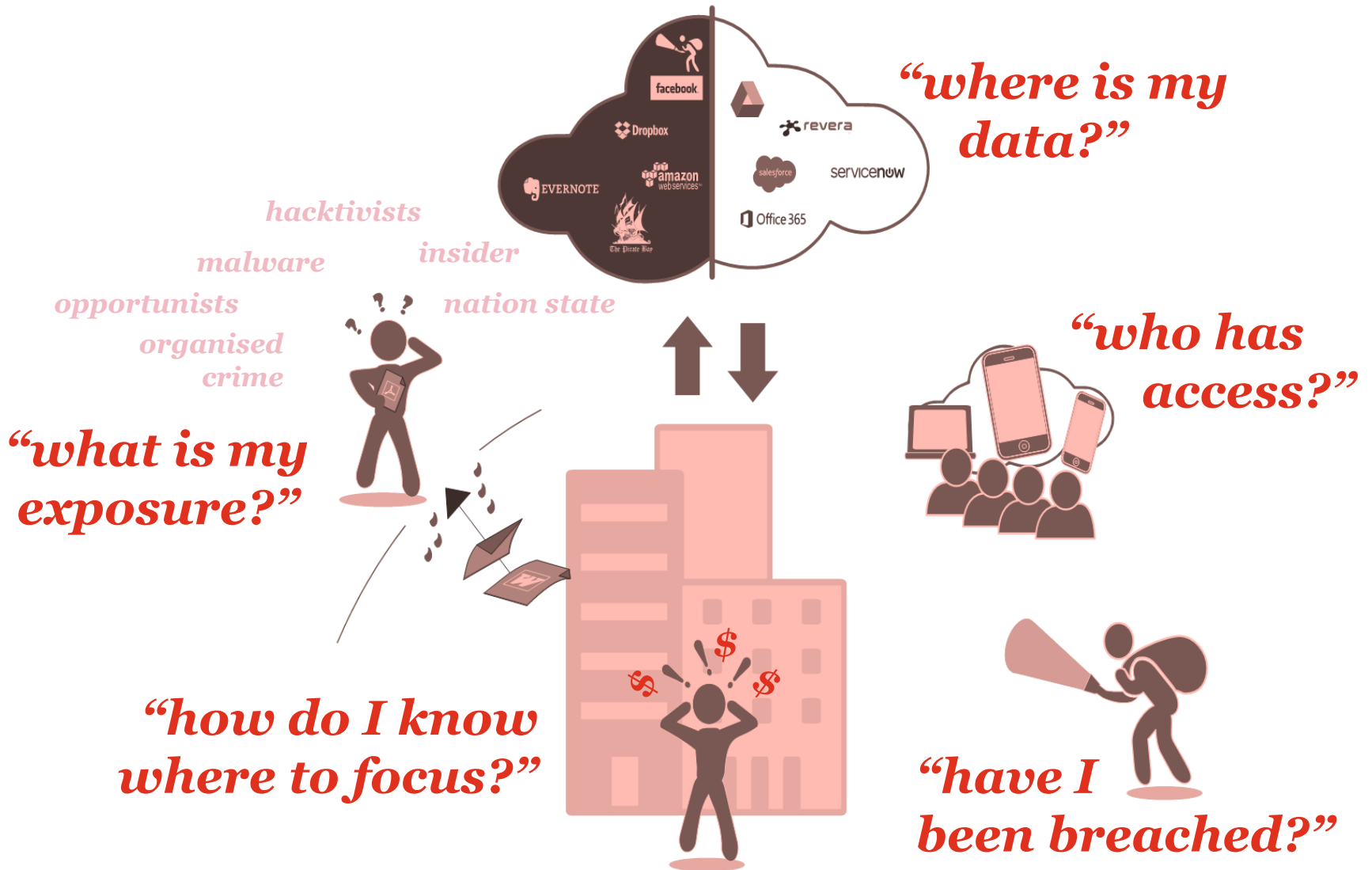
An email from a known sender with a pdf attachment that contained malware was sent to an employee. Upon opening the file, the malware immediately attempted to establish persistent access to the computer.

The hacker attacks weak mail servers to compromise email accounts and send malicious emails to their contacts. The aim is to trick the unsuspected receivers to open the attachment in order to steal their data.

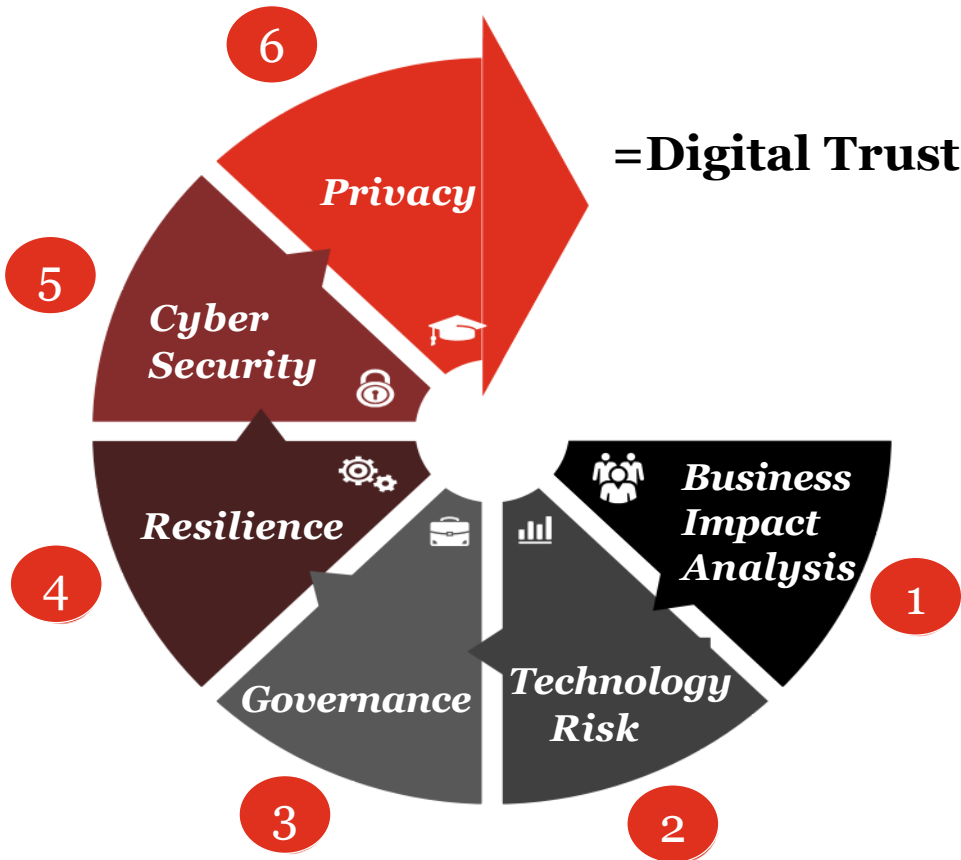
The weak mail server configuration and lack of security software to scan and block malicious attachment make the company susceptible to email attacks. Also lack of filtering internet traffic allowed the hackers to extract and send data to a server under their command.



Questions to consider: What are the risks?



It is impossible to mitigate all risks; instead we need to focus on those with the highest probability and impact



-  1 Identify critical Business Processes and supporting data
-  2 Technology Risks (incl 3rd party risk) threatening the critical business processes
-  3 Define Risk Appetite, Governance and oversight mechanisms including continuous monitoring with metrics
-  4 Build IT resilience capabilities.
-  5 Cyber Security Program design Protect the data
-  6 Build Privacy by design & default and execute Data Cleansing on legacy systems

Top 4 priorities for the Cybersecurity

1. Ensure that you have got **IT security** right
2. Consider cyber security as a **strategic enterprise risk**, not just a technology issue
3. Find out whether you have already been breached, and **pro-actively protect and detect**
4. Ensure that when you are attacked, you can **respond and recover** quickly and effectively



Prevent



Protect



Detect



Respond



Recover

Questions to ask to ensure that you understand your key cyber security risk areas and that you're doing enough



Are you confident in your people?



Are you confident to take risks?



Are you confident in your technology?



Are you confident during a crisis?



Are you confident in your connections?



Are you confident in your priorities?

Thank you

"You can't fight today's threats with yesterday's strategies, what's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries – A Cyber Security model "

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Ltd, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers Ltd . All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Ltd which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.