# Risk strategies

Risk strategies can be followed by the problem owner to reduce a security issue. Risk strategies are part of a broader risk management plan as defined in ISO 27001. Broadly, there are four potential strategies that can be used to handle risk:

1. Avoid risk – circumventing risk; for example by ceasing activities altogether
2. Mitigate risk – Reducing the impact or likelihood (or both) of risk
3. Accept risk – accepting negative (or positive) impact of a risk
4. Transfer risk – outsourcing risk to a third party or parties that manage the risk for you

In the context of the Spamhaus dataset and the three actors (i.e. government, cyber security companies (CSCs) and Internet Service Providers (ISPs)) the potential strategies can be defined as follows:

1. Avoiding risk means:
   1. Government – cutting citizens from the Internet or at least firewalling the country from access to other nations (e.g. like the great firewall of China). Another less rigorous intervention would be only blocking all e-mail related protocols (e.g. POP3, IMAP and SMTP)
   2. CSCs – can advise their clients to stop using e-mail
   3. ISPs – have the technical expertise and blocking power to in fact block all e-mail related protocols from all devices in a certain country
2. Mitigating risk:
   1. Government – Informing citizens, own governmental departments and the private sector about spam and creating awareness of potential threats that can materialize in an impact with certain behaviour of these actors. Furthermore, the government has more stringent and permanent options to consider as the *trias politica* divides jurisdiction in three segments. First, the *legislative branch* is able to create new laws to defend against SPAM. Second, the *executive branch* is able to execute laws that have been passed (e.g. police officers). Third and finally, the *judicial branch* applies laws and convicts individuals and organizations when the law is broken.
   2. CSCs – have (tacit) knowledge to inform companies and other organizations to consult, create awareness and give practical advice how to mitigate cyber risk.
   3. ISPs – can mitigate risk by educating their support staff on SPAM and botnets. Support staff will be better able to detect and give assistance to out of the ordinary computer behaviour when clients describe it (e.g. slower computer phishing, and slow Internet connection). ISPs can also execute a law passed by the *legislative branch* of government, for example to block SPAM or pre-emptively scan e-mails for viruses, malware and worms.
3. Accept risk:
   1. Government – can accept the risk by just letting SPAM happen and leaving citizens and organizations to self-organize
   2. CSCs – can also accept SPAM risk and focus on other forms of risk that might have a higher impact
   3. ISPs – can accept the SPAM risk by leaving customers at their self-organizing power
4. Transfer risk:
   1. Government – could enact a law for customers to share the risk of (im)material damage to customers. This way customers might collectively help each other as shared knowledge about SPAM and its risk directly influences the premium each customer has to pay for the ‘SPAM insurance’.
   2. CSCs – could advise customers on a safer cyber environment and might offer insurance against risk at the principle that a customer must install a minimum amount of security to mitigate risk and if risk nevertheless materialises then is covered by insurance.
   3. ISPs – could also offer customers insurance with the rule that a customer must install a minimum amount of security to be applicable to receive insurance. When a risk materialises in an impact the customer will be covered for damages.

# Other actors influencing security issue

In the previous and this report are defined three actors: government, Cyber Security Companies (CSCs) and internet Service Providers (ISPs). There are many other actors influencing the SPAM security issue. The most important identified for this report are:

1. Botnet masters – are the shepherds of a botnet and access bots via *Command and Control nodes* (C&C’s). Bots will not send SPAM or do anything without an explicit instruction given by a C&C. Destroying the C&C’s immobilizes the shepherds flock. Closing C&C’s is effectively a root-cause solution by both stopping the SPAM and stopping control over botnets.
2. Consumers – are individuals and households that connect to the Internet for information and all kinds of offered services. Consumers are an important actor influencing SPAM security risk. Awareness of consumers means that they could change their behaviour to counter falling victim to SPAM. If less consumers click on the links embedded in SPAM then operating a C&C will not be profitable and thus will a Botnet Master seek his income from other criminal activities.
3. Businesses – are connected to the Internet to create value for customers. Besides consumers also businesses and it personnel can be made aware of SPAM impact and security policies. Moreover businesses should focus on the security of e-mail servers and devices besides merely focussing on whether an application is working.
4. Money mules – are the actors that withdraw money stolen from consumers. C&C’s deposit stolen money in a real bank account. Money mules are random anonymous people that go to an ATM and withdraw the money while withholding a percentage for their service. The money is dropped of at a certain physical location and gathered by the botnet masters. Stopping the recruitment of money mules by botnet masters would be a near root-cause solution as the money does not reach the botnet masters. In addition, Botnet masters do not want to withdraw the money from a bank account themselves in order to stay anonymous.
5. Programmers (malware code writers) – are the actual creators of C&C’s and write the code to infect new devices that, after infection, are added as a bot to a botnet. Stopping botnet code writers from writing botnet related code would also be a root-cause solution. However, this is nearly impossible as every human being has the fundamental right to his privacy at home. Moreover, a malicious person can write the botnet code in the privacy of his home where the privacy is protected by law.
6. NCSC: National Cyber Security Centre – Is part of the Dutch “National Coordinator Counter-terrorism and Security” (Dutch: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)). The NCSC aims at an open, stable and safe information society. NCSC cooperates within an international network of cyber security specialists known as Computer Emergency Response Teams (CERT). The NCSC consists of both private and public organizations which would in principle mean that the NCSC has both production and blocking power to counter SPAM and botnets (Bruijn & Heuvelhof, 2008). The NCSC also creates awareness in the public and private sector.
7. Wombat Security Technologies – Has been chosen as a security leader in the cyber security industry by Gartner (Technologies, 2015). Wombat Security Technologies is focused at creating awareness for its client. Moreover, the focus lies with three core activities (Cyber Security Excellence Awards, 2016). First, learning science principles, second automating attacks and training, and third integrated solutions at minimized cost. Wombat Security Technologies activities transcends mere awareness creation as the company offers the theoretical and practical implementation know-how. Cyber security leaders such as Wombat Security Technologies could have a positive influence at lowering SPAM by lowering botnet infections through awareness and cyber security implementation in booth private and public sectors.

Some actors like botnet masters and botnet programmers play a primary role in the activation and maintenance of a botnet that sends SPAM. Furthermore, money mules are located close to the root-cause of the SPAM problem as they withdraw the stolen money from malicious phishing SPAM and physically bring it to the botnet masters. Consumers and businesses also play their part in the SPAM security issue as they are responsible for clicking on links in (phishing) e-mails and leaving their guard down and not creating and enacting security policies so new botnet infections may occur.

# References

Bruijn, H. d., & Heuvelhof, E. t. (2008). *Management in Networks: On multi-actor decision making.* Abingdon, Canada: Routledge.

Cyber Security Excellence Awards. (2016, February 12). *Wombat Security Technologies*. Retrieved October 12, 2016, from Syber Security Excellence Awards: http://cybersecurity-excellence-awards.com/candidates/wombat-security-technologies/

Technologies, W. S. (2015, October). *Gartner Names Wombat Security a*. Retrieved October 12, 2016, from wombatsecurity.com: https://info.wombatsecurity.com/wombat-named-a-leader-2015