**ESOMAR CEE Forum 2012, Krakow**
**26-27th March 2012**

# FROM TERABYTES TO ARCHETYPES
## The Psychology of Internet Security

Simon Patterson, QRi Consulting, London
Alexander Erofeev, Kaspersky Lab, Moscow

**Abstract**

This paper shows how in-depth Motivational Qualitative Research helped identify the underlying hopes and fears of Consumers in relation to Internet Security. By looking deeply into B2B and B2C Customers' Motivations and Inhibitions within the category, a better understanding was gained of the symbolic and cultural environment surrounding internet security. Using Archetype Theory helped optimise Kaspersky's global brand strategy.

## 1. Introduction

It is estimated that by 2015 there will be 3 Billion Internet users globally. At the same time cyber-crime is an ever present and increasing threat to personal, national and international security, currently costing hundreds of billions of dollars a year globally.

Kaspersky Lab is one of the world's fastest growing and innovative players in the IT Security market (or Antivirus as it is commonly known, although this is no longer a correct definition of its functionality). In 2009 Kaspersky Lab commissioned a study with QRi Consulting (formally CRAM International) to conduct a fundamental piece of Motivational Qualitative Research amongst B2B (IT Security Managers) and B2C Customers. This research was part of a major review of their global brand strategy covering 8 markets (US, UK, China, Russia, Brazil, Germany, UEA, Spain). Due to the rapidly developing nature of this market, a further study was commissioned in 2011 to update the working hypothesis.

Each phase of the research focussed on consumers' hopes, fears, beliefs and stereotypes that drive motivations and inhibitions towards the internet and Internet Security in order to gain better understanding of its symbolic and cultural environment.

Archetype thinking and analysis was utilised at the heart of this research helping reveal untapped hidden feelings, inhibitions and drivers relating to internet use and ultimately in relation to IT Security. Archetype thinking helps to examine and define a brand's image, values and personality. It gives Customers and potential Customers a strong, but often subconscious, indication of their relationships with that brand and for this reason it was used in this study.

By understanding these needs and drivers, it was possible to develop a global brand strategy and strong new positioning that allowed Kaspersky's expansion and to better resonate with its new and growing international audience. In addition, this initial fundamental piece of research would later also help in the areas of product development and communication strategy.

## 2. Project Background

In the last 20 years enormous technological changes have taken place that have reshaped the world. We are now more and more dependent upon the Internet; Tablets and Smartphones are rapidly becoming the norm and dependence upon Cloud computing will escalate at an ever increasing rate. Indeed it has been estimated that:

- by 2013 1 Billion mobile devices will be Online;
- by 2015 there will be nearly 3 billion internet users globally and the number of Network connected devices will be more than 15 billion – twice the world's population.

We increasingly interact with each other, shop and bank online, and store our content, collections & data files on our PCs or in the Cloud. At the same time Cyber-crime is becoming one of the world's biggest threats to personal, national and international Security. Businesses and Consumers are struggling to keep up to date and protect themselves from the latest threats, which can potentially lose valuable data, financial assets and even their identity.

Kaspersky Lab was founded in Moscow by Eugene Kaspersky in 1997. Since then Kaspersky Lab have established themselves as one of the world's fastest growing and innovative players in the IT Security market. During this time the rate of development of technology has been exponential and Kaspersky's superior technical expertise has resulted in the brand's rapid growth into international markets.

## 3. Project Objectives

The objectives of the research were to look into the area of Internet Security and how to communicate with B2B and B2C Customers in this relatively new category that was perceived as both rather functional and low in emotion and often tends to blind the average B2C Customer with science. Indeed evidence suggested that even B2B 'Experts' found the whole area rather rational and functional. Key to the research therefore was the need to understand and uncover the emotional drivers that ultimately are at work in evaluating and making choices and decisions about Internet security across the 8 markets included in the study.

More specifically the objectives were to:

- Elicit perceptions of the Anti-Malware Software (AMS) category overall with a focus on the Kaspersky brand

- Obtain deeper insight about consumer stereotypes and motivations as well as a better understanding of the symbolic and cultural environments of the AMS category in the minds of B2B and B2C Customers with a focus on Kaspersky.
- Get a better understanding of the purchase decision-making process in the AMS, Secure Content and Threat Management (SCTM) category, especially for the B2B segment.

## 4. Research Challenges

Being a relatively new category, there was scope to develop a strong brand image and personality for Kaspersky by identifying B2B and B2C Customers archetypal needs and building on the brand's current perceived image, values and strengths.

IT security is a category that was not particularly engaging or motivating. IT security tends to be seen much like a vaccine. Indeed, after having been inoculated against the threat of potential 'infection', and having taken the precautionary measure, the job is done and B2C Customers in particular tend to suppress their subconscious fears and carry on with their online life as usual.

Indeed for most B2C Customers, it is usually only when purchasing a new PC, laptop or Internet enabled device that IT Security is considered. Further it is usually those Customers who are aware of or have experienced a threat and lost valuable data, financial assets and even personal identity, who have made it their business to become knowledgeable about the category and its brands to avoid 're-infection' in the future.

For B2B Customers it is a far more serious matter that requires their constant vigilance. To be up to date and knowledgeable about threats and brands is crucial for themselves and their companies. Indeed, it was the IT Security Experts who were most aware of Kaspersky and its superior capability. For this reason Kaspersky had become a brand for those 'in the know', a geeks brand that was recommended by experts, but not very well known by B2C Customers, unless of course, they had experienced an IT security problem and sought expert help from a friend or colleague who was in the know.

Kaspersky was in the strong position of having these 'expert recommendations' and credentials. But at the time of the research, it lacked a clear brand image and was relatively unknown in some of the 8 markets, particularly by B2C Customers. From its name it was often seen as a very technical brand, possibly of Russian or Eastern European origin but little else was known about it.

The need for a clear, trustworthy and strong brand image that resonated globally was apparent in order to compete in the International IT security market.

The key methodological concept for structuring our research observations was the theory of "Archetypes" which has been used widely in different social and psychological studies.

Although mentioned as far back as classical and early Christian theological texts, "archetypes" became widely popular from the writings of Swiss psychiatrist and philosopher Karl Gustav Jung (the most notable is Man and His Symbols, 1978). For Jung, archetypes were a form of ancient or archaic images that are driven from the collective unconscious (Fiest J, Friest G, Theories of Personality, N.Y, McGraw Hill, 2009). For him, archetypes were important elements that connect individuals with collective 'memories' (social/cultural interpretations) and also help to explain the workings of the 'dark', unconscious part of human mind.

Although Jung himself tended to see supernatural and even mystical roots of collective archetypes, later authors emphasized the social, linguistic and cultural roots of archetypes. This idea of archetypes has been widely used directly and indirectly in psychology, pedagogy, structural linguistic (e.g. Noam Chomsky) and other disciplines.

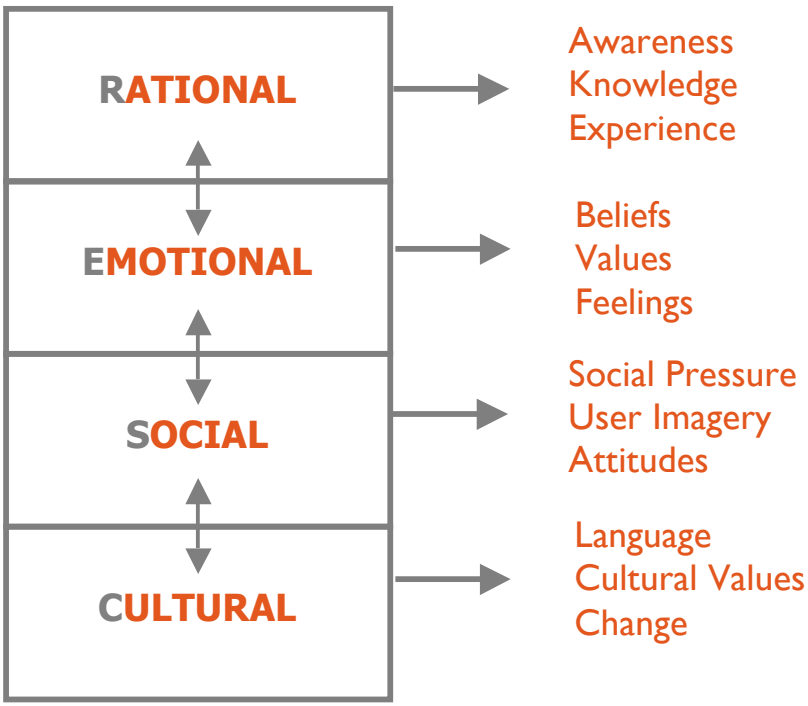
The main areas in consumer research where archetype theory can be usefully employed are in studying human consciousness or behavior that is poorly reflected upon and seldom talked about in the language of daily discourse (as with dreams in Jung's classical studies). In such situations, people still tend to structure their experience but use images and categories coming from deeper and less conscious areas of the mind. Our hypothesis was that IT security was in exactly the same area - where people, although having needs (e.g: for protection) and experience (usually negative after catching an internet virus or other mal-ware) actually have very limited vocabulary, to describe their specific worries and problems. Instead, they have to fall back on more general "fear and safety" related ideas as well as feelings based on classical archetypes.

Whether these archetypes are "Jungian" (so related with collective unconscious, deep-rooted myths and archaic experiences of humankind) or just drawn from associated, intuitively relevant images from out of the mass media, education, primary and secondary socialization etc. is not important, for they have repeatedly been found to be useful and effective. For the purpose of this market research, it was important that the approach was productive and helped us to systematize our perceptions of consumers, without oversimplification or erroneous taxonomies based on professional IT stereotypes about the ways consumers perceive their predicament.

To meet this objective, we used methods based on wide, spontaneous associations and projective visual collages that reveal the insights we needed. These techniques have a long and proved history of usage in qualitative research and are also connected with the method of "associative experiment" developed by Jung and used by him for revealing archetypes.

## 5. Methodology

In order to fulfil the research objectives, it was necessary to understand and uncover not just those rational drivers that B2B and B2C Customers associate with their purchase process, but also the deeper and more hidden Emotional, Social and Cultural drivers that are ultimately at work in making choices and decisions about internet security purchase. See chart below:




To achieve the objectives, a fundamental part of the research was to identify the Archetypal needs that are at play in the minds of B2B and B2C Customers in relation to Internet Security and how these could be utilised in Kaspersky's Global Brand Strategy through a unique and strong image and personality.

As archetypal needs are in the Private, Incommunicable and Inaccessible part of human consciousness (see chart below), projective techniques were used in conjunction with rigorous analysis to elicit these.

| | LEVEL | TECHNIQUE | OUTPUT |
|---|---|---|---|
| PUBLIC | Spontaneous | Simple Questioning | Immediate, Spontaneous. Top of Mind |
| | Reasoned, Conventional | Asking Discussing | Justifications, Explanations Rationalisations |
| | Pre-Conscious | Pressing Reminding | Detailed elaborations/ Introspection |
| PRIVATE | Concealed, Personal | Sympathetic Probing, Empathy, Elicitation | Personal admissions Private wants |
| | Intuitive Imagination Fantasy | Role Play, Collage. Non-Verbal | Symbols, metaphors Latent needs |
| | Unconscious Drivers | Projective approaches. Semiotic Analyses. | Repressed wishes Archetypal needs |

This study consisted of 2 waves:

- The first in 2009, was conducted in 6 global markets; US, China, UK, Germany, Brazil and Russia, and consisted of 4 B2C Customer ECGs (Extended Creativity Groups) and 6 B2B Individual In depth interviews (IDIs) per market.

- The second, in 2011, also covered 6 Consumer markets; US, China, UAE, Germany, Spain and Russia, consisting of 3 B2C Customer ECGs per market and 4 B2B IDIs in US, Russia and Germany.

- Both the B2B interviews and Consumer groups were split between Kaspersky Users and Competitor Users

In order to stand back and be truly objective about the whole area of internet security the interviews were specifically conducted face to face in order to get a real sense of respondent's motivations and inhibitions, emotions, deep rooted fears and anxieties, and help us identify their true wants and needs, through empathic interaction and sensitivity, as well as allowing the local marketing teams to be physically involved in the process. We specifically did not conduct it online, as we wanted to tap more directly into these human aspects and emotions.

Whilst the research methodology was very far reaching in understanding attitudes, behaviour, beliefs and so on, the heart of our analysis was based upon Archetype Theory.

Conventional qualitative research, regardless of whether it is online or in person, can be rather superficial, relying just on what is said, (or tweeted!) and merely descriptive. For this in-depth Motivational research approach, we used many Projective & Enabling Techniques to dig deeper into both B2B and B2C Customers attitudes to understand their inner thoughts and feelings, to help respondents express themselves, and tell stories about their perceived "Ideal" Internet Security Brand, thus helping us to identify the optimum positioning and brand personality for Kaspersky.

It was observed that B2C Customers:

- Are anxious and unsure of what they need to 'defend' themselves against. Threats are often unknown or only partially understood.
- They usually do not know exactly how and where these threats exist.
- This leads to consumer avoidance of delving into the subject themselves as they feel confused, anxious and blinded by science when they do. They try to repress their vulnerability.
- Instead they seek 'Expert' advice from a more experienced friend, family member, colleague or the IT expert at work. They hope for a brand that can provide reassurance.

For B2B 'Experts' it was observed that:

- They are highly aware of risks, especially corporate espionage, destruction or corruption of vital data, system slowing down or breakdown, etc…
- They shoulder much responsibility and fear for their jobs if IT security fails, so they try to make it a shared responsibility with other employees.
- They make rules and restrictions, and impose blocks to reduce threats but these can fail or be circumvented by other employees, leading to unknown risks.
- They are looking for the best possible and most technically savvy IT Security solution that can provide protection and assurance.

Collages were used to explore this further by getting respondents to create an Archetypal 'Visual Story' about their ideal IT Security Brand. From there we explored with them the Characters within these stories and identified the different Archetypes within them. Through this process and the analysis we arrived at 6 Global Archetypal Positionings.

1. **Male/War/Defence** – Good against Evil. Fighting for What's Right – **'The Warrior Archetype'**


2. **Science/Technology** – Leading Edge, Best in Class, One Step Ahead, Technical Excellence – **'The Scientist Archetype'**

3. **Designer/Specialist** – Cool, Cutting Edge, Minimalist, Bespoke – **'The Craftsman Archetype'**


4. **Peace of Mind/Freedom** – Reassurance, Confidence, Carefree, No Worries – **'The Guardian Archetype'**


5. **Magic/Alchemy** – Mystical, Powerful, Insightful – **'The Magician Archetype'**

6. **Female/Protection/Intuition** – Empathic, Alert, Captivating –
**'The Guardian Angel Archetype'**


## 6. Interpreting Archetypes

So what are Archetypes? Archetypes are stories, or characters within stories, which form part of our Collective Unconscious and influence our perceptions, feelings (or intuitions) and decision-making. They are the original forms or personalities or characters that have existed in our psyches from the dawn of time. They are personality “stereotypes” that exist in our unconscious mind and have certain traits and predictable behaviours that can be recognised by us all. Like the characters in children’s stories, fairy tales or even mythology, we can identify these personality types and we see in them typical patterns of behaviour with certain expected outcomes. They resonate with us as they represent patterns of experiences and emotions that, when externalised and personified, help us to identify and characterise situations and how we might deal with them.

Although many attempts have been made to systemise Archetypal thinking there is no set way of determining exactly how many archetypes there are, indeed they are constantly evolving. As Jung, the father of archetypal thinking said himself *“There are as many Archetypes as there are typical situations in life.”* Never-the-less, they exist in all regions, cultures and races, and while archetypes may have different visual expressions and names across cultures, they have shared characteristics that are deep in the unconscious minds of us all.

The use of archetypes in marketing research allows us to go beyond the rational, the normal, the everyday and instead delve deeper into the psyche in order to discover true meaning lurking below the surface of the Customers mind. It is especially relevant to IT Security branding; enabling identification

of how consumers relate to the category and in developing a strong brand identity & personality that satisfies their Subconscious Needs.

Archetype theory was applied in this research to tap into deep-rooted, unconscious needs. From there it was possible to identify what Customers ideally want from a brand; what personality, characteristics and behaviour it should adopt in order to represent their ideal IT Security experience and address their fears and needs in a way that truly resonates.

As a result of using Archetype thinking we identified the optimum archetype for Kaspersky to be “The Guardian Warrior” with elements of the “Magician" and to build stories around this character.

The Guardian

Organised, Systematic, Controlled

**The GUARDIAN** - Preventative and Protecting against threat, Standing Firm, Unflinching, Guarding against intrusion, Ever Alert to deal with problems. His attributes of Organised, Systematic and Control provide Reassurance.

The Warrior

Confident, Powerful, Courageous

**The WARRIOR** - Pro-active, Strikes Back against threats, Ethical and Moral, Seeks Out the Enemy and Destroys it. His attributes of Confidence, Powerfulness and Courageousness provide Peace of Mind.

The Magician

Clever, Analytical, Insightful

**The MAGICIAN** - Sophisticated, Intuitive & Innovative, always able to Create Solutions, is part Scientist (Contemporary Magic). His attributes of Cleverness, Analytical and Insightfulness represent the Magic of Kaspersky that gives consumers faith in the brand to protect them.

## 7. Implementation & Conclusions

The practical implementations of the findings of these qualitative studies were used by Kaspersky Lab in concept testing, the development of research vocabulary for quantitative studies and to describe attitudes and values in the IT Security category.

As has been previously stated, Consumer IT Security is predominantly a low interest and low involved category. In addition, respondents usually have restricted and unstable vocabulary to describe their IT Security concerns and needs. From the point of view of marketing activities and processes this creates substantial difficulties as it limits communication opportunities and decreases the chances of addressing consumers' problems adequately.

Never-the-less, it was expected that the study would help Kaspersky Lab's marketing practitioners to develop a "map of notions and images" based on deeper level concerns and archetypal needs in the IT Security category. Unlike many other product categories where such maps are virtually a "given" and can be easily derived from daily experience, this is not the case for Customers of IT security.

As noted earlier, the six main "archetypes" related to IT safety and security were obtained during the first study in 2009; these archetypes have proved quite stable and, for the most part, were reproduced in the second study. Although more solid and academic research efforts are required to make sure that we are dealing with a stable structure deeply embedded into European consumers' minds, it has proved to be a good working model which has since been used for the elaboration of several business strategies in the areas of product, communication and branding.

For product strategy, the fact of heterogeneity of customers' needs stimulated us to think about the wider product portfolio which can address different needs. As a result Kaspersky Lab has evolved from solo offering to a multiple products strategy, with new products such as Kaspersky PURE and ONE that have been launched recently.

Communication and brand strategies have been affected the most. Key Brand values and personality have been rectified and reconstructed based on the chosen Protector/Guardian Warrior archetype. Emotional messages (both visual and verbal) have been mainly aligned with the most potent archetypes which have allowed campaigns to be differentiated for different products.

Also worth noting is that the research has had a solid educational and enlightenment value - it has helped marketing people within Kaspersky Lab to orientate themselves within this category and understand specific needs and stereotypes related with B2C Customers' IT Security needs.

Another important application of these results was in B2B marketing. Probably the most important learning here was that whilst corporate

customers and individual consumers are very different in terms of their knowledge, needs and behavior, they share a similar system of "archetypes". Therefore one can develop a single brand for IT security based on the same emotional benefits, with only functional messages being differentiated depending on products alone. This approach has helped to improve consistency in communication efforts and also significantly optimise brand investments.

An illustration of how Kaspersky are using these deep insights is their new Sponsorship of the Ferrari F1 Team where the Warrior Guardian Archetype, with a touch of Magic is clear to see:


Another example is advertising for Kaspersky Pure, using the Guardian Angel Archetype:

## 8. **Acknowledgements and References**

Acknowledgements

Peter Cooper (1936-2010)
Special thanks to James Patterson, and also to Jessica Neild.
Edited by Dr. Alan Branthwaite

References

Campbell J (1949), *Hero with a Thousand Faces*, Pantheon Books

Chomsky, Noam (1968), *Language and Mind,* Harcourt, Brace & World

Cooper P & Patterson S (2000), *The Trickster – A Theory of Modern Branding & Advertising"*, Excellence in International Research 2000 – ESOMAR

Fiest J & Friest G (2009), *Theories of Personality*, N.Y, McGraw Hill

Jung C G (1972), *Four Archetypes,* Routledge & Kegan Paul

Jung C G (1959), *The Archetypes and the Collective Unconscious*, Routledge & Kegan Paul, Ltd

Jung C G (1964), *Man and his Symbols*, Aldus Books

Lannon J & Cooper P (1983), *Humanistic Advertising: A Holistic Cultural Perspective,* Seminar on Effective Advertising, ESOMAR

Mark M & Pearson C S (2001), *The Hero and the Outlaw,* Mc Graw-Hill

Pawle, John (2000), *A new view of global Brand Personality for the Millennium.* Market Research Society Conference

Vogler (1998), *The Writer's Journey*, Sheridan Books