ANALYSIS OF INFORMATION THREATS AND COUNTERACTIONS IN CONSUMER ORIENTED ORGANIZATIONS
(SEPARATING THE BEST FROM THE REST)

Tamara Jovanov, a post-graduate student in the field of Marketing on the Faculty of Economy at the University "St. Ciril and Metodius", Skopje; Curently – a volunteer in the field of Statistics on the Faculty of Economy at the University "Goce Delcev", Stip, Republic of Macedonia

Generation Y, what do they really want? It's the 21st century and the greatest consumers of information ever are on roll. Consumers are emrasing a digital lifestyle and enterprises are interacting in new ways. In times like this, when the informations are the companies most valuable resource, the issue about informations threats and security should be their top priority. With opportunities come risks and protection is about more than just technology, it's about people, process and technology. While some companies are struggling to survive, others are rethinking their business strategies and redesigning the marketing practices to build more profitable, enduring relationships with their customers.

No one is safe! There is a moment in an individuals or corporations life where they allow themselves to think that they can rest and catch a breath, but it is the moment they chose not to think any more.
When Henry Ford brought affordable automobiles to the average citizen in 1908, he also improved the fortunes of criminals by ushering in Crime 1.0 – technology – assisted crime. Speeding away in their Model Ts, bank robbers and other undesirables were harder to catch. Fast forward a century, the computer is the 21st century equivalent of last century's car, and with it we enter Crime 2.0 – high technology – assisted crime. Cybercrime is estimated to be a $105 billion market that will continue to grow as the complexity of cybercrimes intensifies.[1] Customers, especially businesses, are starting to use security as a discriminator and therefore, security has become a nonnegotiable expectation of business cooperation and long-lasting relationships. Successful marketers are moving beyond the traditional practice of outbound marketing (trade shows, seminar series, email blasts to purchased lists, internal cold calling, outsourced telemarketing and advertising), where the marketer pushes his message out far and wide, hoping that it resonates with that needle in the haystack to inbound marketing (blogs, ebooks, white papers, viral youtube videos, Search Engine Optimatization – SEO, webinars, feeds, Really Simple Syndication - RSS) that helps in finding people who already are learning about and shopping in the specific industry. It is time to shift to a new marketing strategy that targets the masses of people who are trying to block the large amount of outbound marketing interruptions in more and more creative ways (with caller id, spam filtering, Tivo and Sirius satellite radio) and be found by customers, rather than searching for them. The big picture is to turn a corporations website into its own lake of honey for the awoken and hungy "bears". Regarding this new proactive way of doing business built on technology basis, the shifting IT environment must be taken in consideration, thus, it's the main reason why security is becoming one of the most important issues in companies development. The technology shift embraces the fundamentall change of software communications – many transaction occur over the web – Service Oriented Architecture (SOA), AJAX; The network defenses that are covering a shrinking portion of the attack surface; The legacy code that is being widely exposed; The security model that has changed from good guys vs. bad guys to enabling partial trust – there are more levels of access – extranets, partner access, customer access, identity management; The social networking that gives attackers access to much more personal and product information, etc. With a glance on the history and evolution of marketing, agitation, propaganda and information warfare, it's noticeable that the risks and the threats to information systems have multiplied and are addressing problems such as analyzing threats as defacing, hacking, cracking, intrusion, denial of service attacks, viruses, Trojan horses, key logger, shock measures, eavesdropping, surveillance, espionage, fake proposals of goods and services, scams related to payment cards and accounts of electronic payment systems, cyberwar and netwar. As an answer to the high level

[1] www.Business-standard.com, January 03, 2008

security solutions, the cybercriminals are both, leveraging new technologies to propagate cybercrime as well as reinventing forms of social engineering to cleverly ensnare consumers and businesses. For example, the tools and technologies used to create the interactive nature of popular social networking sites have become a land mine for cybercrime. The fast-flux technique is an additional example of criminals abusing technology developments. Fast-flux is a domain-name-server (DNS) switching mechanism that combines peer-to-peer networking, distributed command and control, Web-based load-balancing, and proxy redirection to hide phishing delivery sites. Fast-flux helps phishing sites stay up for longer periods to lure more victims. High-profile Web sites are also highly targeted. Cybercriminals are increasingly targeting more affluent users, such as C-level executives who represent a small number of wealthy, high-level individuals in positions of power to gain access to larger bank accounts, login credentials, or even email addresses that spam an entire organization. Social engineering is the key attack method, with more sophisticated tricks evolving on daily basis. Cyber criminals are focusing mainly on events such as the Olympics, the election season, football and other sporting events and the holiday season. Cybercriminals are targeting newly discovered vulnerabilities in "third-party" software applications, such as QuickTime, RealPlayer, Adobe Flash, etc. As is occurring now, both spam and phishing are a part in blended threats, as well as bots and botnets that are an important part in the threat chain for spamming, information stealing, targeted attacks and large-scale attack campaigns. It is obvious that there is a problem that needs to be taken care of and as a part of the solution can be some of the following strategies for information security:

- Valuate corporate assets smarter (i.e. what are they worth to an attacker?)
- Adopting risk management approaches that identify high – value targets and then do threat modeling to determine how those targets can be reached;
- Build strong systems that appear strong when viewed by an attacker (i.e. design for defense in depth);
- Valuate customer data beyond what is currently protected;
- Planning changes in privacy requirements and legislation that addresses stored data like “pet’s name”;
- Planning for new requirements on data disposal;
- Use standards – based approaches with multiple vendors;
- Ingrain security awareness into the culture;
- Build a perimeterless network, moving to Network Access Control (NAC), to gain user – focused control;
- Stop being event driven;
- Spend more time investigating procedures than technology;
- Embrace the attacker and think like him/her to succeed.

Cyber crime is on the attack, and it can happen to anyone. If you think this has nothing to do with you, you are mistaken. If you have a bank account, this kind of thing impacts you. If you have a phone, this kind of thing impacts out. If you have a name, and we all have names, your name can be stolen and somebody can take that identity and get credit cards in your behalf…

What is becoming increasingly clear is that the companies that will apply some of the mentioned counteractions on information threats are the ones that will be widening the gap between themselves and their less savvy competition. By exploring new ways to refine their marketing approaches, work collaboratively with all of their enterprise-wide departments and enhance the security and richness of each and every customer interaction, they are already pushing their inbound initiatives to new lengths in an attempt to uncover the next best practices that will provide competitive differentiation. At some point, the distance between the best and the rest will become impossible to recover. Forward-thinking companies have come to realize that the time to invest in winning strategies and best practices for greater customer information security is now.