Global Cyber Security Summit – Rome, Italy, Oct 31st-Nov 1st, 2016

So much has been said and written about Cyber-Security these past weeks and months that it's difficult to determine whether it's real or sureal. With an estimated 175,000 cyber attacks per day (PwC report) at a total cost to business of $315 billion in the 12-months ending in Septembre 2015 (Financial Times), cyber crime is more than a corporate nightmare.

Last month, the company DYN informed authorities that they had been victim of several massive DDoS (Distributed Denial of Services) cyber attacks involving tens of millions of IP addresses executed through a botnet consisting of a large number of Internet-connected devices—simple every-day products such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware. With an estimated load of 1.2 terabits per second, the attack is, according to experts, the largest DDoS attack on record.

Earlier this year, Yahoo! announced that 500 million client accounts had been hacked. Other recent high-profile malignant attacks include Red October, TV5Monde, Operation Olympic Games, Paris G20 Summit, Google, Sony Pictures, Playstation, Visa, Subway, Target, Anthem and many more. As the victims names indicate, cyber attacks are not focused on any specific industry, sector, nationality or country.

A cyber-attack is "any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system".

Cercle Montesquieu Members Laure Lavorel (CA Tech) and Eric Gardner de Béville (The Client Relations Company) were speakers at the Cyber Security Summit in Rome, Italy, organized by Skytop Strategies and sponsored by the Law Firm Latham & Watkins on 31st October-1st Novembre 2016. The conference was a high-profile gathering of Cyber specialists including U.S. Homeland Security, insurance consultants, high-tech companies, communication agencies, law firms, cyber-service providers, corporate in-house General Counsel and other corporate executives concerned about the rising risk of cyber attacks aimed at their business.

Topics of discussion included cross-border cooperation reflecting difficulties pertaining to the current fragmented regulation instead of a "think global, act local" approach that underlines the need for U.S., EU and other national authorities to implement regulation that is local in enforcement but that also captures the global reach of cyber crime. It was highlighted that the global cooperation is also made more difficult by the fact that U.S. tech companies dominate the tech-world. Companies such as Google have a more dominant position in the EU than the U.S, and Facebook has more European users than Americans. Mention was made to the World economic Forum cybercrime recommendations establishing a neutral forum based on a public/private partnership that should drive a better cooperation against cybercrime. Main goal is to encourage the adoption of the Budapest convention (first international treaty on crimes committed via the Internet) and get more common legislation (harmonization of domestic criminal substantive law elements) and international cooperation in law enforcement investigations relating to cybercrime.

Also of interest were the presentations and discussions on corporate preparedness and responsiveness to cyber attacks with illustrative examples such as the TalkTalk cyber attack in the UK where company management responded quickly to inform local police but delayed informing the UK governement cyber control authorities, or the Yahoo! attack where the company considered the

attacker to be a “sophisticated country-sponsored actor” and kept the attack secret for almost two years.

Of growing interest is the fact that cyber security is becoming a high-profil area of concern to corporate management as witnessed by the increasing number of CISOs (Chief Information Services Officers) and the strong focus by corporate and legal management on cyber issues of all kinds. Executive Search professionals are increasingly looking into cyber security experience as a differentiating characteristic between top candidates for the General Counsel, CEOs and COO positions.

With IOT (Internet Of Things) becoming a corporate buzz word and a household name as more and more every-day products are becoming internet connected –such as cars, TVs, coffee perculators, washing machines, refrigerators- cyber risk is growing exponentially. Today the central issue of combating cyber crime is not so much how to prevent it from coming “in” as it is to keep if from going “out”.

Indeed, more and more experts agree that there is no 100% prevention solution and that the big issue today is how to contain the cyber attaker once he’s in and especially prevent him from going out to disrupt corporate, client and customer reputation and relations.

Cyber Security insurance is also a hot topic these days and it’s perhaps not a great surprise that financial wizzard and investor Warren Buffett has recently entered the cyber insurance market…Insurers are focusing more and more on advising and indeed requiring their clients to have comprehensive internal resiliency plans to ensure best-in-class preparedness and immediate-execution contingency measures to minimize the global risks to business posed by cyber crime today.

And with the European Directive on security of network and information systems (NIS Directive) that entered into force in August 2016 and will have to be transposed by Member States by May 2018, cybersecurity-related obligations and liabilities of “operators of essential services” will increase and force companies to prevent cyber attacks, prepare for remediation and incentivize them to subscribe to cyber insurances.