SPEAKER SPOTLIGHT: **FREDERIC VIRMONT**

Cyber Security Expert, Merck

Cyber attacks have continued to be a threat to the pharmaceutical industry. Could you give us a little background on why the industry is such a prime target?

Hackers are looking for a company's most valuable and sensitive data. This includes elements like clinical data, Intellectual Property, formulas for compounds, and in some cases patient or employee personal data as well. The amount of money that a hacker can get for a stolen proprietary formula on the black market significantly eclipses what they might be able to get for something like stolen credit card information. They'll target industries that yield bigger payouts than they would get by going after someone like a private citizen via identity theft. The cost of stolen credit card data on the black market is roughly $13-$21. The cost of an EMR (Electronic Medical Record) is ten times more.

In your experience, what have been the key challenges to ensuring network security in Pharma?

Investments in Cyber Security: Despite news of companies being breached, there are still companies who do not spend enough in Cyber Security. Applying a "crown Jewels" approach: Companies have sometime difficulties to identify their most critical systems and to protect them. The "crown Jewels" approach is a way to prioritize efforts and budget.

Another big challenge in Pharma is protecting laboratories systems, which use to run on special hardware and OS (sometime old version of Windows). They are therefore difficult to update or upgrade.

Security Awareness training: Security Awareness training must be efficient and given on regular basis. This means ensuring the content is up to date and practical enough so that people can apply what they learn but also understand the consequences of their behavior for the whole company.

Frederic Virmont, Cyber Security Expert, Merck

Frederic has worked for Merck KGaA for the last 10 years. Passionate about Cyber Security, he has been working and involved in a lot of topics around security, like Risk management and Cloud Security. Frederic built and led the whole Vulnerability Management program at Merck. He is currently leading the Penetration testing program.

How do you see these challenges being overcome?

Management support: The management, at all levels, should support all Security Activities. The Security Department should be perceived as Business enabler and not as Show stopper. That means accompanying the Business and showing them the added value of Cyber Security. That also means providing solutions instead of problems.

DRP: Companies must ensure they have SLAs for DRP (Disaster Recovery Process) for their most critical systems and they must test the recovery process at least once a year. (best practice). DRP is the answer of many security problematics. People sometime forget that Availability is also a security matter (Confidentiality, Integrity, Availability).

What does your role as a Cyber Security expert in Merck entail?

My role as Cyber Security Expert is to protect Merck Business against current and up-coming threats. I managed the global Vulnerability management program, (3 millions of IP scanned monthly), and I'm currently responsible of the Penetration testing program. But I provide a different kind of support regarding security topics, both technical and non-technical, to many teams.