Interview with Troels Oerting on cybersecurity in modern organizations

February 12, 2016 By Pierluigi Paganini

An interview with Troels Oerting on the cyber security in modern organizations and the importance of the role of the Chief Information Security Officer.

The role of the chief information security officer (CISO) has profoundly changed over the years, from IT security management to high-level risk management.

Today a CISO is a crucial figure in any organisation, so I decided to discuss the topic with one of the professionals that most of all have contributed in the recent years to the security Industry, Mr Troels Oerting.

Mr. Oerting has more than 35 years experience in Law Enforcement, he is former Director of Danish NCIS, National Crime Squad, SOCA and Director of

Cybercrime Centre (EC3) and Head of Europol's Counter Terrorism and Financial Intelligence Centre.

Today Troels Oerting is the Chief Information Security Officer (CISO) at Barclays, I consider him a Master, in my opinion, only a few professionals have had its experience in cyber security, Troels is the incarnation of the modern CISO.

How has the role of the CISO changed in the last years?

In the past, which is not so long ago, I believe that the CISO role was considered to be a technical role. The profile should be technical and it would often report to the Operations & Technology chief in any bigger organisation. The role was rather reactive and aiming at 'ticking' boxes in auditors control schemes based on various vulnerabilities. I think you will find that there is a growing understanding for the fact that the CISO role is not a tech role but a wider business role. Cyber security is a 'trust' issue, and trust is what customers, regulators and citizens want. And cyber security is not a 'tech' issue that can be solved with more firewalls or anti-virus products. Contrary to a technical outage that can be mitigated by flying in a new device to replace the broken one, cyber incidents are manmade. They change form and shape faster than light and adapt to new control measures. With more than 250,000 new malware variations every day and new techniques, tools and procedures we can not only control us out of cyber intrusion. It requires an adaptable flexible intelligence led organisation that can predict new threats and not 'just' address what has hit us.

What are the principal threats for modern

organisations?

When we, in Barclays, assess the threat we first identify our Adversaries. Who are they? We have intrusion attempts from Nation States, Organised cybercriminal networks and hacktivists. Next in our assessment is to have a look at the Intent of each of the Adversaries. Do they want money, IPR, sensitive information, wipe the estate, blackmail us and when we have a good overview on that, we then zoom in on their tools they use to obtain their goals. After determining the threat we now take a look at our defence. Where are our vulnerabilities? Where are our 'crown jewels'? What are our controls? Based on these principles we constantly adapt to the change in threat by increasing controls, tighten our protection of our Crown Jewels and minimise our vulnerabilities. The threats are multiple from mainstream daily attacks, malware campaigns, phishing attempts, DDoS attacks, APT, Trojans etc. We aim to be able to Predict, Prevent, Protect, React and Recover.

Which is the economic impact of the cyber security in your organisation? Do you consider it satisfactory?

I am never satisfied if we have losses. Regardless if it is losses of sensitive data, money or other valuables in our digital repository. We lose money and we lose data and we strive to drive them to zero, but that is not possible in a global bank operating in 50 countries with 50,000,000 customers and 140,000 employees. But we take our customers and employees security and privacy very, very seriously and work tirelessly to prevent and protect.

What do you suggest the executive management do to improve the overall security of their organisations?

I think that the executive management already have a full understanding of digital security. I believe that trust is key, and we will be measured by our

customers, society and regulators if we can keep their trust. Banks are known for being able to take care of their customers valuables, savings and salary – and this can be transferred to our future digital economy and digital identity. We will continue to keep our digital assets safe, and my executive level have full understanding for that fact, and support me every day in keeping the bank safe.

Let me thank Mr Troels Oerting and his staff for this interview.

Pierluigi Paganini

(Security Affairs – CISO, Troels Oerting)

banking | CISO | cyber security | cyber threats | Hacking

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a

Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

US Intelligence confirms the ISIS used chemical weapons

NEXT ARTICLE

A replica of AlphaBay market used to steal login credentials

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

Security Affairs newsletter Round 47 – News of the week

February 14, 2016 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

1. Network Security Solutions 

2. Business Network Security 

3. Security Risks 

4. Information Security Program 

5. Top IT Security 

6. Network Security Map 

7. Top Network Security 

8. Network Security Breach 

Back to top