Cyber Security & Resilience Roadshow

Cyber security and Cyber resilience are hot topics. Driven by the growing importance of, and dependency upon information technology, and fueled by high profile, highly damaging security breaches that make news headlines. In the latest IT Trends study by the Society for Information management it scores number 1 on the list of CIO worries.

In response to this growing need Glenfis, a strategic ATO of Axelos and a well established IT service management consulting company, together with Axelos and GamingWorks organized the first Cyber Security and Resilience Roadshow in Zurich. The roadshow sessions are aimed at capturing key issues facing organizations and exploring how Resilia® can help provide solutions.

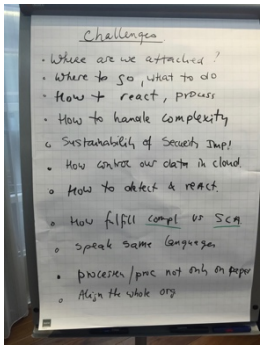
'Resilia®' is the latest addition to the Axelos best practice portfolio, developed to '*help organizations improve their cyber resilience and protect themselves from cyber-attack'*. The focus of Axelos is '*Putting people at the centre of organizational cyber resilience'*.

As **Peter Hepworth, CEO Axelos** stated ' *Cyber crime is increasingly recognized as one of the most serious risks to a strong global economy, market reputations and to national security'* adding that Resilia® will equip people with '*knowledge and confidence to deal with cyber security risks*'. Axelos is strongly positioning the PEOPLE side of the PPT (People, Process, Technology) equation. As **Nick Wilding**, head of Cyber Resilience at Axelos also stated '*Inside any organization there is a powerful force that can help protect their reputation, safeguard their information and keep customers close – people*'.

However, it is also the people who leave memory sticks containing sensitive data in their cars, who succumb to spam mails and who stick their passwords under their keyboards. It is people who circumvent security policy to 'get their job done'.

The latest Cybersecurity findings from Cisco also reveals that attackers are shifting their emphasis from '…*seeking to compromise servers and operating systems to seeking to exploit users*'.

The Roadshow event



12 Security professionals attended the session. Martin Andenmatten from Glenfis and Dan Cole from Axelos opened the session.

Jan Schilt from GamingWorks first captured the challenges of the participants.

The delegates then took part in the Ocean's 99 cybersecurity business simulation. In the simulation they could apply their 'security best practices' and at the same time explore recognized issues and experiment with using Resilia® guidance and recommendations.

Ocean's 99 Business simulation

In this simulation game: *"The owner of the Bank of Tokyo has decided to exhibit three world renowned objects. The 'Star of Africa', the 'Jewish Bride' and a 'Bugatti 59'. The challenge for the team is to bring the objects to Tokyo, on time, safely and securely, and to have them exhibited, however there*

are rumours that Ocean's 99 a criminal organization wants to steal the objects… In the game the various stakeholders make use of information systems for planning, for managing, for transporting, for monitoring the objects and for booking and selling tickets, there are many opportunities for Ocean's 99 to exploit vulnerabilities.

During game preparation the delegates must design a security policy and strategy, perform a risk assessment and invest in security countermeasures. Then the game starts and the objects must be transported to Tokyo. Are the countermeasures good enough to prevent Ocean's 99 to attack? If an attack occurs how quickly can the team detect and respond?

In the simulation game the delegates were confronted with numerous threats and attempts to gain access to information so that Ocean's 99 could steal the objects. The team had to apply best practices, and ensure everybody maintained security discipline.

At the end of the simulation delegates were asked '**Which issues in this game do you recognize as the top 3 that need solving in YOUR organization**'?

- Overall awareness, not just IT (4)
- The need for clear procedures and processes (4)
- Communication (3)
- Overall clear roles and responsibilities(3)
- Good service design with focus on security (2)
- Teamwork in case of security issues, leadership(2)
- Decision makers know their role and responsibilities
- Business involvement and commitment
- Finding balance between SLA and Compliance
- Proactive behaviours, thinking ahead
- Assessment, Where are we? Are we safe?

Delegates were asked "Would this type of event help you gain senior management commitment to cyber security"? 70% agreed it would, however 30% thought not. Either because top managers were already engaged or because 'senior management has delegated this' – ***as can be seen in recent scandals, board room awareness and commitment is critical. It is not something that can be delegated away. EVERYBODY has a responsibility for Cybersecurity and Resilience***.

100% of the delegates found that the use of a simulation is a powerful way of bringing people together (across the delivery chain) to create awareness. It clearly shows the importance of roles and responsibilities; allows people to see, feel and experience from different perspectives - such as business & IT, management and operational; it clearly demonstrates the need for a holistic approach (People, Process, Product, Partner); It shows the need for balancing opportunity against risks – which is why senior commitment is mandatory in helping shape policy and influence priority and decision making.

Finally, we asked the delegates '**what were YOUR personal learning outcomes'**?

- Recognized the importance of communication and training of crisis situations, even more after this session
- Experiencing a different role
- Experiencing how it feels if procedures are keeping me from doing my job
- The relationship between the project organization (project manager) and CISO
- The need to go back and to review our internal procedures, are they still fit for purpose
- Integrating RESILIA into ITSM
- Always be suspicious, improve your procedures
- With good roles and clear definitions it will be easier to deal with serious issues
- Invest more time in the beginning of projects or new services

Quotes:
"Keep calm and maintain oversight also under pressure"

"It was very interesting to take another role than usual and view from another perspective, thank you!"

"Good way to raise awareness about the complexity of information security"

"Very valuable, good fun, lots of experts involved"

"Very good seminar and very valuable. Good to see the importance of a SPOC"

"No real AHA discovery but a good session to memorize again the importance of having up to date systems in place"

"The Cyber Resilia gearbox (collaboration, mechanics, pitfalls, communications, etc.)"

"Balance between opportunities and risks. And the different attitudes that came together in a (project) organisation"

"Employment awareness is important; this interactive way is a perfect way of developing this"

"Cyber Resilience is nowadays one of the most important and indispensable capabilities for responsible corporate management. Ocean's 99 is an ideal instrument to promote awareness and understanding of the central cyber resilience measures at all levels and to sustainably anchor them. For Glenfis OCEAN's 99 is a strategically important product in our security advisory and training portfolio". Martin Andenmatten - Glenfis

"I am always surprised how experts learn from interactive learning. It shows that the learning process of experts is based on the 70-20-10 rules. 70% of the learning by experts takes place during tough projects, interaction with other experts and by experimenting. Today was a great example". Jan Schilt – GamingWorks.

"Good organizational cyber resilience requires people to have the right practical skills to implement best practice. Interactive learning and simulations are a vital part of that personal development – and Oceans99 demonstrated an ideal environment for everyone to test their skills. The learning from the experience should make everyone more effective in their contributing to good cyber resilience." Dan Cole - AXELOS