Regional Training Centre at Zurich International School

Title: "Cyber Security: What your School Needs to Know...and Do!"
Schedule: Thursday, 11th October 2018 - 08:30 - 16:00
Training Location: Zurich International School (ZIS), Steinacherstrasse 140, 8820 Wädenswil, Switzerland

Time	Agenda Item
08:30 - 09:00	**Meet and greet**
09:00 - 09:15	**Welcome and initial introduction** 1. Attendees to outline objectives for the day 2. Overview of the day
09:15 - 10:15	**"Adequate security" is mandated by law - What this means in the context of:** 1. The General Data Protection Regulations (AR 25/ 32) 2. European Data Protection Board (WP29) 3. ISO27001 4. Codes of Conduct: a. ISO27001/27002 b. NIST c. NCSC 10 Steps
10:15 - 10:30	**Break**
10:30 - 12:00	**Cyber Security at your School - What are the threats and probability of being a victim?** **Recent school examples of:** 1. Criminal student fee fraud 2. Malicious student attack 3. Sextortion attack 4. Numerous phishing campaigns 5. Internal Ddos Attack, triggered by Student/Staff **Workshop** Cyber Activity 1 - Evaluating your organisations risk and susceptibility to a Cyber Attack
12:00 - 12:30	**Lunch**
12:30 - 14:00	**Cyber Security Testing & Risk Management** 1. How do you reduce these attack vectors? 2. How can you ratify the measures you have in place? 3. Technical and Vulnerability Penetration Testing a. Internal b. External c. Web Application d. Phishing 4. Review of example outputs

	5. Checklist - “Operational Steps to Mitigate Cyber Security Risks” a. Maintenance of a cyber security risk log b. Scheduled update & patch management c. Regular penetration testing d. Phishing Campaigns e. Staff cyber awareness training 6. Discuss any events at your school, what did you do? How did it affect your school?
14:00 - 14:15	**Break**
14:15 -14:45	**Cyber Security IT Compliance Projects** 1. Mobile Device Management (MDM) 2. 2FA and ID Management 3. Network Monitoring 4. System Updates / Patch Management 5. Anti Phishing, Anti Malware protection 6. Data Loss Prevention (DLP) 7. Cyber Awareness Training 8. Cyber Security Incident Management
14:45 - 15:30	**Embedding cyber protections at your school** 1. Cyber awareness and phishing susceptibility at your school 2. GAP analysis and fostering a security conscious staff base 3. Review of systems and services against the 10 Steps to Cyber Security 4. Demonstrate due-diligence by assessing the systems and services vulnerabilities through appropriate penetration testing and analysis 5. NCSC Cyber Essentials and the ISO27002 codes (leading to ISO27001 compliance)
15:30 - 16:00	**Collaborative Wrap Up** 1. Q&A 2. Lessons learned - feedback from 9ine 3. The road to a strong security posture - aims and goals 4. Future 9ine Regional Training Events

For information on joining, email cameron.strange@9ine.uk.com