Digital Risk & Safety (Cyber Crime)

David Appleyard, Apple36 Consulting Ltd (in place of David Benford), Blackstage Forensics Ltd

David referred to 'digital leakage' and advised that companies should look at the risks which apply to their particular type of business and how serious any threats could be. Consider what the pay-off would be for a cyber criminal hacking into your systems. What do they stand to gain from it? Once you understand their motivations, then you can begin to consider ways of reducing the risks or making yourselves less of a target by making it more difficult for the criminal to get into your systems.

David referred to the Iranian nuclear facility which was hacked using clever cyber techniques which closed it down. Hacking into something such as a water facility or big businesses such as Boeing or Rolls Royce could also have major consequences. Hackers may be after data or set to damage a brand's reputation.

Hackers are often criminals who simply do not like the concept of big business and want to cause as much mischief as they can. In some areas of the world hacking is even state-sponsored eg China, Vietnam.

In this digital age there is a tendency for people and employees to 'overshare' information, often without any awareness of the possible consequences. People may - intentionally or unintentionally - reveal sensitive and potentially damaging business information. The fact that many of the technologies use geo-data to determine the location of a user poses an added threat.

David illustrated the dangers by showing examples of one person's postings, which although at first appeared to be innocent actually led to a lot of personal information being traceable. The person had initially posted a photograph of his temporary contractor's badge from the site where he was working (a breach of security for the company as their badges could now be copied).

By using a software programme that can track a person's postings it was further revealed that this person worked for the RAF as he had posted pictures of himself in uniform. He had also left a trail of his activities via other postings which gave away his location, including his address where he had ordered a pizza to be delivered. Google Street View enables anyone to see the actual location/ property and estate agent information can even reveal the layout of the interior! Staff need to be educated and discouraged from revealing business information and information that could jeopardise their own security.

Staff who, for example, are in the business of transporting money could be under threat if they inadvertently reveal their location information to criminals. This could lead to robbery or kidnap en-route.

David said there are companies who will help discover how vulnerable you are as a business to cyber crime but warned that some eg whose services are free could potentially unleash their own rogue software

David's advice in a nutshell

- Understand your business and why it could be targeted

- Identify the risks

- Realise that avoidance is impossible, but make yourself less of a target

- Educate staff - be careful what is in e-mails and what they post on Facebook, Instagram etc.

Other safeguards

- Use strong passwords – change often. Don't write down, put in a computer file or reveal to others.

- Don't click on links to rogue sites – always look at the address you are being sent to.

- Don't open a email – particularly an attachment or a link - if email sender, etc is not recognised.

- Be alert to rogue callers etc you offering their 'help' after there has been a cyber crime reported in the press.

- Have good anti-virus software on your systems to detect malware.