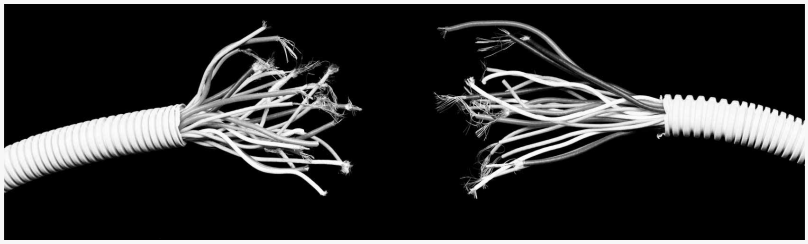
Are firms taking too many risks with their security by being Cyber-risk centric?

There is a real concern that physical security is getting overlooked and underfunded. Does this make firm more susceptible to hacking and espionage?



Are firms taking too many risks by being Cyber-centric?

Getting espionage on the agenda is highly important in every firm.

LONDON, UNITED KINGDOM, October 5, 2018 /EINPresswire.com/ -- This week's revelation that operatives from the Russian intelligence GRU have been involved in wholesale hacking of sensitive targets, prompts the question about technology in the workplace, our use of this technology and our understanding of how it should fit with physical security.

The gap between physical and technical security is widening, not helped by Board level executives being blinkered by the Cyber threat. So, are companies putting themselves, their personnel and their assets at risk due to this focus?
Security guards are, in many companies the lowest qualified and the lowest paid personnel. Physical security is very often thrown in with cleaning and facilities management.

For sure Cyber Security practitioners are specialist in their chosen fields, many have college and degree level educations and attend regular training as part of their Continued Professional Development (CPD), while most security guards will not do any refresher training or CDP at any time during their careers.

> Are security managers being pressurized by their Boards into prioritizing Cyber Security?"
>
> *Alex Bomberg*

Physical security has become the weakest link and exposes flaws that can be further exploited by social engineering and by technical means.

As a society will have become far too reliant on technology without properly understanding its correct usage or in some cases, emerging media or technologies.

Social Media for example is one of the biggest risks to corporate security today. It's ironic that companies will spend so much money on security, yet

not be concerned with what staff put on Social Media or even what their own PR teams put out at times.

To understand the issues of social media risk, you must first understand and identify what information might be sensitive or how innocent information might be used in social engineering to gain other information… For the determined espionage aficionado, just knowing someone is out of the office is enough of a starting point.

The same can be said for the use of mobile devices in the workplace. An area not that well shored-up in most small and medium-sized firms, yet this area presents massive sensitive data issues if the loss of a device or breach via a device should occur.

The space where physical and technical security first meet, is often with access control and CCTV systems. Most major office building now make use of these systems, some of which are extremely sophisticated.

Even at entry level, these are expensive systems that if used correctly will enhance the overall security. The issue lies in the fact that those operating the systems either:

- Lack the training, qualification or licensing to operate the systems.
- Are not motivated to follow policies and procedures when operating these systems.

The two above examples both come down to bad management or poor budgeting. But another area of concern is the serviceability of the equipment installed – if the equipment is not working correctly, then it's no use to anyone.

A great example of failings where it comes to basic physical security are:

- Staff skill fade
- Bad moral and non-incentivized staff
- No (qualified) management or ownership for internal security.
- Throwing money at systems (that are not going to be properly utilized after the initial enthusiasm)
- No regular auditing or review of security systems and personnel

"CCTV or any other technical counter-measure, is only as effective as the personnel using it!"

It would really surprise most employees of a company who utilize physical security services that they receive very little training to become licensed and are not required to carry out any refresher training, apart from first aid training.

Security Officers are in a very trusted position, in most cases they also have full unrestricted access to a facility and this, most often than not, includes after hours. This is concerning given that for services that are supplied by a third-party contractor, no due diligence or checks are carried out periodically on either the supplier in question or on the security staff it employs.

Quality control is obviously the answer if you know what questions to ask in the first instance. In the UK for example, a sperate Security Industry Authority License (SIA License) is required for guarding and CCTV operators. Many end-users are unaware that this is a legal requirement until something goes badly wrong. For example, if a CCTV operator is required to give evidence in court and it is later realized that he or she is unlicensed and unqualified, then the case falls apart. That is a good example of why checks and measures are needed.

It is important for firms to know if they are getting value for money from a security service provider. Guards are often individuals who do not have a college-level education, they are often paid not much more than the minimum wage…

So, what is the answer?

Firstly, firms must have a security audit conducted by a competent and qualified individual, ideally an external source. The audit must jointly cover physical and technical security holistically and if required, a penetration test should be carried out to expose flaws.

Based on that audit, recommendations can be acted upon, but an audit/review process needs to be put in place. The most important thing is, however, ownership of overall security within an organization, it is the fact that security is not “Joined up” that gets exploited by those carrying out espionage. Increasing the counter espionage capability of any organization or firm is always a benefit - just getting the espionage risk

Alex Bomberg is the CEO of International Intelligence Limited and has delivered lectures on the subject of counter espionage for many years. International Intelligence Limited is a UK based specialist provider of Intelligence and Counter-Intelligence services, including Counter Espionage.

The company was founded in 2002 and provides services to commercial and governmental clients globally.

Alex Bomberg
International Intelligence Limited
+44 207 7911627
email us here
Visit us on social media:
Facebook
Twitter
Google+
LinkedIn
