Arthur J. Gallagher

SECURITY BREACH PLANNING

FAQs

SECURITY BREACH PLANNING

FAQs

Cyber generally, and the area of data breaches particularly, are growing concerns for organisations, with the ever increasing awareness of such incidents and the high profile media coverage that can follow.

Sarah Hewitt, a Director in the Major Risks Practice of Arthur J. Gallagher and Nick Bellamy, a Senior INT Specialist with Chubb Risk Engineering Services look at some of the questions which often arise concerning security breach planning.

Why do you need Breach Response Plans?

Cyber-attack is now a fact of business life – at some stage most businesses will have to deal with being attacked. The UK Government 2015 IS Breach Survey found that 90% of large and 74% of small businesses had a security breach in 2015.

Of paramount importance to a business is how quickly and effectively they can react. The aim of a breach response plan is to mitigate response times and control/reduce the impact of a breach.

The speed of response and effectiveness of actions taken following a breach are a window to a business and will dramatically affect how they are perceived in the aftermath.

What about the impact of the forthcoming EU GDPR?

The new EU General Data Protection Regulation has now been signed off and, following a grace period, will come into force during May 2018. Failure to comply will result in fines - up to 4% of the global annual turnover, which eclipse the current maximum fine in the UK of £500,000.

Breach prevention & detection

Prevention is far better than reaction so you should already have in place a full ISMS including Data/Asset identification and classification and risk assessment to identify appropriate protections - both technological and human – deemed necessary.

Speed is of the essence when it comes to detection as the longer the attackers have access to your system the greater the amount of data they can steal or system damage they can do.

What should a Plan include?

The plan should be similar to a Disaster Recovery or Business Continuity Plan with a pre appointed team, emergency contact numbers, prepared forms and processes.

A plan should include detailed procedures and activities, supported by appropriate document templates to allow a systematic and logical reaction to the breach. The plan should include the following sections:

A. **Breach Containment**
B. **Impact Assessment**
C. **Recovery**
D. **Notification/Communication**
E. **Evaluation**

It should be predetermined who will do what – roles and responsibilities must be detailed in the plan and supporting document templates produced.

Summary

Breach Response Planning is now a mission critical activity which will help you to comply with the legislative implications of the inevitable breach, protect your reputation and ensure business continuity to protect revenues.

FOR MORE INFORMATION CONTACT:

Sarah Hewitt
Director
Major Risks Practice

T: +44 (0)20 3425 3317
E: Sarah_Hewitt@ajg.com
www.ajginternational.com

Arthur J. Gallagher