final

RefTech Issues Anti Cyber Attack Check List

Following last Friday's global cyber attack, RefTech a leading supplier of event technology, has compiled a checklist for individuals and companies to follow to help them reduce the risk of future attacks.

Simon Clayton, chief ideas officer, RefTech said: "Friday's cyber attack hit on a global scale, and is set to escalate this week as more companies discover that they have also been affected. The repercussions of the attack are likely to continue for some time; it is a massive demonstration of what can happen if you are not security conscious and highlights that even the biggest organisations are vulnerable. Our check list below sets out simple steps that will help individuals and companies reduce the risk of future attacks of this nature."

On your personal computer:

1. Make sure you install operating system updates when they're made available
2. Make sure you have good anti-virus software installed and it's regularly updated
3. Backup all the data on your computer regularly
4. Never open an email attachment that you're not expecting even if it seems to be from a reliable source such as tax authorities, banks, delivery companies and so on
5. Never click on a web link in an email from an unknown contact
6. Make sure your passwords are strong*
7. Use a different password for each online system you use
8. If you're offered two factor authentication for using an online system, use it

If you run a company your IT system is almost certainly too important for you to be able to say 'We have an IT manager – all this stuff is their responsibility'. You need to be as involved in this as you are in other activities that the business depends on for its survival. Specifically, you need to:

1. Take IT security seriously. Imagine what would happen to your company if your computer network was knocked out for a couple days. Worse still, what would happen if you lost all of the company data and couldn't recover it?
2. Make sure a named individual in the company has the clear responsibility for backing up your systems at least every night
3. Make sure they are doing it

4. Make sure they test the backups regularly to prove that the backups can be used if the worst happens
5. Make sure a named individual in the company has the clear responsibility for updating your PC and servers' operating systems
6. Make sure they're doing it
7. Make sure that every computer that's linked to your network (including computers not owned by the company) has the latest security patches installed
8. Make sure all those computers have good anti-virus software installed and that it's kept up to date
9. Make sure everybody in the company follows point 4 to 8 above

*For more information about how to create a strong password, please download RefTech's free white paper: http://www.reftech.com/passwords.php

For more information on data protection, please download RefTech's free white paper titled: 'Data Protection in the Events Industry: what you need to know to stay within the law' https://www.eventreference.com/promo-www/datasafety/download.php

(ends)