MindLink

6 Reasons why using WhatsApp at work is risky business

1 billion users and counting. What makes for some impressive numbers when it comes to user adoption and pervasiveness, may well be the downfall of many a business.
Employees are blurring the line between private life and work by bringing consumer apps into the workplace. 35% are now using WhatsApp & Co to share sensitive business information and documents.

Let's have a look why letting employees use WhatsApp, WeChat and other social messaging apps, may put your enterprise at risk.

1) It's a Consumer Tool

Easy to sign up to, easy to share and free to use – consumer tools are built on the principle of pervasiveness. Many of them hence live in the world of 'Shadow IT' ie. they are being used without the consent or even without the knowledge of the employer, which has security implications and counteracts the idea of having universally accessibly tools for all employees. (the consequences are knowledge silos & lessened economies of scale)

2) It has no enterprise-grade data security or privacy

If you are in doubt to what extent you are putting your company data at risk, here are the latest news:

- Jan 2016: Hackers are designing custom malware for WhatsApp
- Sept 2015: 25 most popular apps to have been infected by malware - list includes… WeChat
- June 2015: WhatsApp ranked worst for users' data privacy

WhatsApp is cloud based with little security controls or data protection. Corporate requirements such as Private Cloud or On Premise deployment, MDM/EMM support for mobile devices (so that you can remotely lock or wipe devices if lost or stolen), authentication or user/access management are not supported. Know-you-third-party #KY3P principles are equally lax, meaning companies don't know who they are sharing the same platform with to communicate and store data.

3) It offers no data compliance

For everyone in regulated industries such as financial services (but also for companies with strong self-governance principles), adhering to regulatory rules is a must. Compliance and archiving features are not supported by consumer or social tools, yet the ability to monitor, store and search communication channels is a requirement for most corporates today.

4) You can't connect it to your business systems

WhatsApp & Co are standalone tools; another app on your desktop or mobile screen so to say. They don't integrate with your enterprise tools to send data into and out of chat rooms: your CRM, Email, SharePoint etc. Yet, bringing all your tools together creates efficiencies, allows for better decision making and saves you time by avoiding the 'log on/log off' scenario.

5) It doesn't integrate with your UC tools

Again efficiencies are lost by not being able to combine your messaging applications with your already existing Unified Communications platforms such as Microsoft Lync/Skype for Business, creating knowledge silos and inefficient workflows.

6) It creates Cross Industry System Risk (CISR)

Here are some of the realities when using consumer/social chat apps:

1. Lax information security, data control & privacy
2. Sensitive business data is being shared (e.g. board reports, financials, trade secrets, legal documentation, HR files...)
3. No KY3P principles - firms don't know who they are sharing the chat platform with (criminals, terrorists or other undesirable elements)

Combine the above facts and the risk associated with using these tools is substantial - not just for your business but for any business sharing their corporate IP on consumer/social platforms.

It's crucial to give your staff access to tools they want whilst maintaining control and ownership from a corporate perspective. Enterprise-ready messaging applications, built from the ground up for corporate use, are a sound and efficient alternative.

For more information contact: info@mindlinksoft.com