2023.5.1

中国风险消息<2023. No. 1>

聊天软件在公司业务中的风险和对策

【要点】

- ◆ 介绍日企管理层对于以微信为代表的聊天软件在公司业务中的意见和现实情况。
- ◆ 从总体概况、现状、使用场景等方面分析聊天软件在公司业务中使用的整体情况。
- ◆ 从信息泄漏、网络安全、软件程序 3 个风险角度，结合实际案例，阐述聊天软件在公司业务中的具体风险，提出建议性措施，以预防和降低公司的信息泄漏事故发生的概率。

1. 是否可以禁止在业务中使用聊天软件（日本企业的烦恼）

1）聊天软件的介绍

聊天软件是通过电脑或手机进行社交和信息传播的应用程序。员工往往倾向于可以随时通过手机进行实时通信，采用对话的形式进行沟通交流，更快捷高效地推进工作。而传统的商业电子邮件仅是单方面发送电子邮件，沟通效率不高。此外，也可以很容易创建群组，并与多个人共享信息，发送和接收图像和视频也很简单。

在中国，聊天软件不仅在日常生活中不可或缺，而且也作为商业通信工具大范围使用。其中“微信”是最广泛传播的聊天软件之一。

2）聊天软件在公司业务中的风险

在与公司内外的联络中，日本公司更倾向于使用公司设定的电子邮件地址进行正式的商务交流，而不是使用聊天软件。邮件传播具有信息记录、整理和备份等优势，能够提供可追溯性，方便后续查证和跟进。另外，邮件还可以通过附件的形式发送文件、合同等文档，并且可以采取附件加密的安全措施，让信息更加规范和安全。

另一方面，在中国的许多公司（包括日本公司）中，习惯于通过聊天软件与公司外部的合作伙伴进行通信，并且发送和接收与业务相关的文件（在与客户的第一次会面中，经常看到交换聊天软件 ID 而不是名片的场景）。在许多情况下，由于使用个人帐户，因此管理员难以掌握沟通的内容和发送接收的文件内容。聊天软件不仅限制了字数，而且也没有邮件的备份和记录功能，容易导致沟通过程中信息的遗漏和不确定性。

因此，如果公司允许聊天软件在业务中使用（包括默认），重要信息可能会无意中在发送和接收聊天信息时发生泄露。除了错误发送等的人为失误以外，在聊天过程中很有可能出现故意或者恶意地发送和接收重要信息，并且员工离职时，将原公司的现有客户的信息带出等现象。此外，对于管理员来说，很难随时掌握聊天内容，因此即使有员工长期消极怠工，不及时联络客户，也无法进行适当的管理。

3）是否应该禁止在业务中使用聊天软件

由于公司业务中使用聊天软件存在各种风险，因此在中国的日本公司中，很多管理层希望禁止使用。并且实际上已经有部分公司规定了禁止在公司业务中使用聊天软件。然而，鉴于中国目前的商业习惯，“禁止业务中使用聊天软件”的规则很难生效。以“微信”为代表的聊天软件深入渗透到人们的生活中，即使我方仅使用公司邮件发送信息，但也会收到来自客户的聊天软件的回复，或者客户直接要求“希望用聊天软件而不是公司邮件发送资料”。如果不考虑此类实际使用情况，直接规定禁止将聊天软件下载至公司电脑，或者禁止通过手机在业务中使用聊天软件，则可能会导致在公司内部使用聊天软件的员工数量继续增加。

因此，为了采取符合实际情况的安全措施，而不是统一禁止使用聊天软件，对公司来说，现实的对策是应该告知员工聊天软件在业务使用相关的风险，并制定在使用中应遵守的最低限度的规则。

2. 使用聊天软件的风险和案例

1）聊天软件的概况和现状

近年来，随着移动互联网和智能化技术的不断发展，微信、钉钉等聊天软件在企业日常办公中得到了广泛的应用。这些软件提供了高效、便捷、实时的信息交流和协同办公功能，也能作为企业的宣传和广告的手段。

以下表格展示国内主要平台型聊天软件的现状信息。

表 1 主要平台型聊天软件

产品	开发公司	定位	活跃用户数量
WeChat 微信	腾讯	用户之间，与企业之间的信息交流；宣传和推广	13.13 亿①
DingTalk 钉钉	阿里巴巴	流程简化，注重流程管控。	6 亿、企业组织 2300 万②
Lark 飞书	字节跳动	对内沟通，重点解决日程管理、文档协作	611 万③

① 数据来源：http://stock.hexun.com/2023-03-22/208055173.html

② 数据来源：www.ithome.com/0/664/012.htm

③ 数据来源：https://36kr.com/newsflashes/1699631220506629

聊天软件在公司业务中的使用场景如下所示。

表 2 聊天软件的使用场景

场景	详细内容
团队合作	许多团队使用聊天软件来协调任务和共享信息，特别是对不同地区或时区的团队来说，这是一种方便和高效的通信方式。
内部协作	员工可以通过聊天软件快速交流和分享信息，例如发送日程安排、查看工作进度、提供反馈等等。
客户沟通	许多公司使用聊天软件与客户进行互动和沟通，包括传输文件、发送产品信息、提供技术支持、处理订单等业务。
品牌推广	大多数公司也将聊天软件用作品牌宣传和营销推广的渠道之一，通过发布文章、设置微信小程序、展示产品信息等方式吸引受众的注意。

随着聊天软件的使用越来越广泛，安全问题也成为人们日常关注的一大问题，比如，员工可能通过聊天软件向外泄漏公司机密信息、进行虚假宣传或欺诈行为，而企业也面临着数据安全、隐私保护和管理规范等方面的挑战。

2）公司风险

员工在工作中使用聊天软件，可能会对公司造成以下多种风险：

① 信息泄漏风险

聊天软件不同于面向大众的网站、微博，仅公众号、视频号等少数功能可以开放给其他人，而主要的通信功能等则表现出一定的私密性。很多员工将这种私密性等同于安全性，使用聊天软件办公时比较随意，这是信息泄漏事件发生的重要原因。实际上，聊天软件的基本属性就是开放性，所有信息都要在公开的网络上传输、存储。

泄露信息的员工个人毫无疑问需要承担相应的民事或刑事责任，但同时，公司会受到更大的影响，被政府处罚，停止业务或处以罚款，并导致市场信誉下降，丢失用户等间接损失。

案例：

- 2017 年，某银行从业人员通过聊天软件向他人透露客户个人信息，被监管机构查处，并被要求进行整改。
- 2018 年，某医疗机构的医生在聊天软件群里发布了患者的病历，导致患者隐私沦为众人谈资。
- 2020 年 11 月，某快递公司的五位员工以每日 500 元的价格将自己的公司内部账号租借给不法分子进入物流系统盗取用户信息，包括发件人地址、姓名、电话以及收件人电话、姓名、地址等。被泄露的信息数量超过 40 万条，涉案金额达 120 余万元。
- 2022 年 4 月某市市委组织部工作人员曾某，收到上级单位下发的一份秘密级文件，要求紧急传达落实。因需要阅办的领导外出不在，曾某为尽快将文件传达到位，遮盖文件密级标志进行扫描，将电子版发送至单位聊天软件工作群，造成泄密。

② 网络攻击风险

聊天软件作为主要的社交应用程序，其用户规模庞大且具有高度互联性，存在很高的网络攻击风险。

黑客会通过多种方式攻击聊天软件，获取邮箱地址、名字、业务内容等关键信息，进而攻击公司内部网络，盗取保密资料。同时，保密资料泄露，还可能在网络上形成舆情事件，大大影响公司的声誉。

表 3 主要网络攻击风险（公司）

风险	详细内容
安全漏洞	任何软件都有可能存在安全漏洞，这些漏洞可能导致黑客利用聊天软件程序中的相关接口和功能来进行攻击、病毒传播或者数据泄漏等。
远程代码漏洞	远程代码执行漏洞可以允许攻击者执行恶意代码，从而控制被攻击者的设备、窃取敏感信息等。
恶意软件攻击	黑客可能通过聊天软件平台向用户发送恶意链接、文件或软件等，从而在用户的计算机上安装恶意软件，对其进行攻击、窃取信息或远程控制等。
社交工程攻击	黑客可能利用社交工程技术来欺骗用户泄漏自己的聊天软件帐号和密码，或者通过冒充用户身份来诱骗其他用户共享敏感信息，导致帐号被盗或者其他安全问题。
网络钓鱼攻击	黑客可能伪造聊天软件官方网站或者发送伪造的聊天软件系统消息或邮件，诱骗用户输入自己的帐号密码或点击恶意链接，从而造成损失或泄漏敏感信息。
聊天软件小程序	在使用小程序的过程中，姓名、地理位置、出生日期等个人信息泄漏的情况时有发生，这意味着一旦黑客对其进行攻击，将很容易获取相关信息。此外，利用图文识别聊天软件小程序转换文件，图文转换过程中相关文件内容已经被上传到互联网服务器上，对公司信息安全造成危害。
文件传输助手	聊天软件的“文件传输助手”表面上是移动设备之间的信息互传，实际上这些文件已经保存在设备以及互联网上，通过技术手段即可进行复原。聊天软件登录的 PC 端会进行自动备份，点开相关文件夹就能看到完整内容。如果粗心大意忘记清理备份，那么相关信息将面临泄漏风险。

案例：

- 2018 年 4 月份，某科技公司曾被发现存在聊天软件钓鱼攻击事件。攻击者通过伪造聊天软件界面，利用社交工程手段引诱员工点击恶意链接，从而导致一部分员工账户和密码被盗取，信息泄漏风险严重。
- 某头部金融服务平台的小程序在 8 月推出了“邀好友，千元好物一元购”的活动，可以邀请好友给自己助力砍价，商品价格最多可以砍到一元。活动刚开始，黑客就迅速完成了自动化攻击工具的开发，导致平台给出的优惠全部落入黑客之手。
- 2020 年 2 月，某市属企业收到 1 份机密级文件，该企业行政部主管将文件交彭某办理，彭某虽知涉密文件禁止使用手机拍摄、传输，但为图方便，仍使用聊天软件小程序中的一款图文识别小程序对文件进行扫描，转换为文字后，通过数据线传输方式，将文本导入非涉密计算机中处理。但不久后，该聊天软件小程序后台运维人员从服务器中非法获取文件图片，并将其上传至互联网，造成严重泄密。案件发生后，该运维人员被追究法律责任，彭某被给予党纪处分、扣薪处理。
- 2021 年 3 月，某区工作人员施某看到同一办公室收文人员接收到上级党委 1 份内部文件后，用手机拍摄该文件，通过聊天软件点对点方式发送给某银行工作人员何某，何某接收到图片后，将文件编号截去，通过聊天软件点对点方式发送给某公司职员徐某，徐某又将该图片发送至同学聊天软件群，从而引发该内部文件在网上大范围扩散、炒作，给相关工作造成极大被动。案件发生后，施某、何某受到党内严重警告、行政记过处分，徐某受到行政警告处分，其他相关人员也受到了处分。

2）个人风险

个人在使用聊天软件时，如果没有采取安全措施，也同样存在很多风险。

表 3 主要网络攻击风险（个人）

风险	详细内容
帐号被盗	黑客可以通过钓鱼网站、恶意软件等各种手段窃取用户的聊天软件帐号信息，进而获取用户的个人信息、聊天记录以及访问权限等敏感信息。
用户隐私风险	聊天软件在使用时需要获取相应的权限，包括获取照片、麦克风、位置等信息，如果存在未授权的访问或滥用的风险，则可能导致用户隐私泄漏或遭受其他危害。
金钱盗取	黑客通过发送诈骗信息、病毒等方式，窃取聊天软件的支付密码，将用户余额转移到其他账户中。

案例：

- 2019 年 7 月，A 女士在聊天软件上收到一条诈骗信息，声称其银行卡被冻结，需要解冻操作。陈女士根据提示，输入了支付密码，并给对方转账 8800 元。警方通过调查，发现骗子在该案中使用了“钓鱼网站”的方式进行诈骗。骗子设置了一个假的银行页面，要求用户输入银行卡信息以验证身份，骗子可以通过这些信息迅速将用户钱包里的钱转走。
- 2019 年 8 月，B 先生在社交媒体上公开了一个聊天软件群聊的截图，称在广州某处停车场发现了数百辆共享单车堆放在一起，有人在该群里提供地址和密码，让其他人可以去该停车场取车。很快，这条消息引发了广泛关注和讨论，但实际上这些小黄车都已经报废，并早就已经被相关方面处理了。该聊天软件截图是通过黑客手段获得的，并非相关人员主动公开的。这就意味着，个人聊天软件信息被黑客窃取并泄露，导致了不必要的舆情和误会。

3. 聊天软件的风险对策

从以下五个方面说明在业务中使用聊天软件时的风险对策。

(1)硬件对策

在业务上使用聊天软件时，推荐专门为业务开发的具备多种安全功能的聊天软件。例如：企业微信、钉钉。这些软件的安全功能如表 5 所示。

表 5 工作专用聊天软件的安全功能

聊天软件	安全功能	安全认证
企业微信	在传输和存储过程中，对内部数据进行加密处理。	ISO 27001 信息安全管理体系认证
	通过指纹、面部识别、OTP 等安全认证方式，确保没有认证的用户无法访问。	中国等级保护三级认证
	针对部门和员工设置不同的数据权限。	C5 认证，德国联邦信息安全办公室（BSI）发布的云服务安全认证标准
	在设备丢失后，可以远程销毁数据。	/
钉钉	登录账号时，需要输入用户名和密码，并通过短信验证码等二次验证方式进行身份验证。	ISO27001 安全管理体系认证
	使用数据加密技术，保证用户消息在传输和存储过程中不会被窃取或篡改。	CMMI5 评级认证
	支持管理员对组织架构、权限角色、APP 应用、部门等信息进行严格的管理和控制	国家商务部保密备案
	对日常操作、账户行为、客户端版本等进行监测和分析，并在发现异常行为时立即进行告警和处理。	/

2）软件方面

仅靠硬件对策无法完全防范信息泄漏和网络攻击。因此，采取与硬件对策配套的软件对策是很重要的。有必要制定有关员工行为、信息管理、设备使用等的规则，并通知员工。

软件对策（公司内部规则制定等）的重点如表 6 所示。

表 6 软件对策（公司内部规则制定等）的重点

风险对策	详细内容
发送信息要求	聊天软件的工作群应指定专人作为管理员，交流内容严格限定为周知性的一般信息，禁止传播国家秘密、工作秘密、客户信息、商业秘密以及个人身份证件等信息。
数据分级	针对不同类型的数据给出不同的保密等级，并对不同保密等级的数据采取相应的安全措施，如禁止用聊天软件传输、加密、备份等，以确保数据的机密性和完整性。
权限管理	通过加强访问权限管理，限制用户访问不必要的数据。管理员需要根据各种角色和职责，对用户的访问进行精细化管理，确保每个人只能访问必要的信息，避免信息泄漏风险。
密码保护	防止账号被盗，保护聊天软件登录密码和支付密码。设置强密码，包括数字、字母、符号等。定期更换密码，不要使用相同的密码用于多个账户。不要在公共场合或不安全的网络环境下输入密码。启用密码保护功能，如聊天软件的手势密码等。
禁用公共 Wifi	避免在公共场合、未经验证的 Wi-Fi 网络、未加密的 WiFi 网络、使用简单密码的 WiFi 上登录聊天软件。这些网络都可能被网络管理员或黑客截获、破解和窃取信息数据。
禁止点击未知链接	不要随意点击聊天软件上的广告、推销商品的链接，并在必要时使用反病毒程序扫描系统以确保安全。配置聊天软件隐私设置，禁用“漂流瓶”、“摇一摇”、“附近的人”，防止未知人员寻找到账号。
日志审查	通过实时监控系统日志，分析日志数据，发现系统中的异常操作行为。还可以根据预设的规则和标准，自动监测、识别、报告潜在安全事件，快速响应网络安全问题。

3）应急响应对策

由于很难完全预防信息泄露和网络攻击，因此有必要考虑应急响应对策，应对紧急情况，防止损失进一步扩大。以下说明重点。

表 7 应急响应的重点

风险对策	详细内容
①检测	规定应该报告的“异常”的定义、报告路径。
②初始响应	明确关闭受感染的设备和网络的操作流程，并设置关闭系统和停止网络的判断标准。设定向总公司、机关、公安报告的条件。
③调查与分析	明确原因调查和影响范围的特定流程。并制定启用外部专家的判断标准。确定受损信息的重要性和对业务的影响。
④信息披露和道歉	整理对外发布的判断标准、应对外发布的项目，整理对信息泄漏等受损客户的应对方针和应对要领。
⑤恢复和防止复发	不仅要考虑系统数据的恢复策略，还要考虑防止再次发生的措施。

4）日常的教育训练措施

虽然软件制度都已经制定，但员工的安全意识不强，无法落实，导致网络攻击时间发生的案例也很多。因此平时应该加强对员工的教育培训，并定期进行各种网络安全训练。

表 8 员工的教育培训重点

风险对策	详细内容
安全教育	由内部员工或外部专业机构定期开展网络安全、信息泄漏等相关专题讲座，全体员工参与，并进行调查测试，普及安全知识，提高员工安全意识和技能，降低人为因素造成的信息泄漏风险。
专项检查	定期开展自查及抽查工作，将聊天软件电脑使用情况、工作群管理情况、信息发布保密审查纳入重点检查内容。
钓鱼攻击训练	通过聊天软件平台向员工发送模拟钓鱼电子链接或其他形式的电子通信，测试员工的警惕性和反应能力。通过这种方式，员工可以更好地认识到网络钓鱼攻击的危害，并学会如何防范和应对。
网络攻击模拟训练	通过模拟网络攻击来检测和评估企业网络安全体系及其响应能力。

5）个人安全对策

由于个人聊天软件的安全事故也频繁发生，因此员工同样需要采取安全对策进行防范。

表 9 个人安全对策的重点

风险对策	详细内容
更新版本	及时升级手机系统和软件可以修复已知漏洞，提高安全性。尽量避免对手机进行 Root 或越狱操作。
安装应用	下载应用时，只使用官方应用商店或其他可信渠道下载应用程序。在安装任何应用前，仔细检查应用程序请求访问的权限，特别注意隐私相关的权限。
电脑防护	对于安装聊天软件 PC 版的电脑，同样要采取安全措施：安装杀毒软件和防火墙、不使用公共电脑登陆、及时更新操作系统和应用程序和注意聊天软件程序的登陆异常等安全警报。

4. 总结

在本文中，根据中国发生的信息泄露和网络攻击的案例，解释了公司应采取的对策重点。这些案例的主要原因是软件的技术缺陷，人为错误等。为了采取措施应对这些风险，有必要进行全方面的商讨和推进，包括技术方面、管理方面、操作规则方面、法律方面等。希望本文中提到的措施，有助于安全地使用聊天软件并导致信息安全事故的减少。

全文完

参考资料：

1. 和讯网新闻：http://stock.hexun.com/2023-03-22/208055173.html
2. IT 之家新闻： https://www.ithome.com/0/664/012.htm
3. 36 氪： https://36kr.com/newsflashes/1699631220506629
4. 网易新闻：https://www.163.com/dy/article/HMFNQMM00514D3UH.html
5. 搜狐新闻：https://www.sohu.com/a/492876948_161795
6. 保密观”微信公众号：微信泄密又出新案例 https://www.12371.cn/2021/11/19/ARTI1637277436721109.shtml
7. 永安在线报告：基于微信小程序生态体系的黑灰产研究报告 https://zhuanlan.zhihu.com/p/408514439

执笔：瑛得管理咨询（上海）有限公司　咨询部 张若亭

MS&AD InterRisk综研隶属于MS&AD保险集团控股株式会社，是一家专门从事风险管理有关的调查研究以及咨询相关的专业公司。有关咨询方面的洽谈可以联系我公司下述联络方式或是联系三井住友海上、爱和谊日生同和各营业担当。

联系方式　㈱ MS&AD InterRisk综研　综合企画部 国际业务组
TEL.03-5296-8920　　http://www.irric.co.jp/

瑛得管理咨询（上海）有限公司是在中国上海设立的隶属于ＭＳ＆ＡＤ保险集团的风险管理公司，主要提供诸如工厂/仓库的风险查勘、BCP 计划的制定等各种风险相关的咨询服务。如欲联系或申请等请联系下述地址。

联系方式　瑛得管理咨询（上海）有限公司　（日语：インターリスク上海）
上海市浦東新区世纪大道 100 号　环球金融中心 34 层 T10 室-2
TEL:+86-(0)21-6841-0611（代表）