从“字节跳动”前实习生篡改代码攻击大模型训练说起——商业秘密和网络安全

作者：杨迅

近期，多家媒体披露了一起严重事件：前字节跳动实习生田某某涉嫌通过编写和篡改代码等手段，恶意破坏公司的研究项目模型训练任务，造成重大资源浪费。2024 年 11 月，字节跳动已向北京市海淀区人民法院提起诉讼，索赔侵权损失 800 万元及合理费用 2 万元。此事件紧随某律所实习生泄露拟 IPO 企业商业机密案之后，不仅凸显了加强实习生管理的紧迫性，也为所有企业敲响了商业秘密保护和数据安全的警钟。

一. 商业秘密保护：不仅仅是字面上的保护

谈及商业秘密保护，大家往往想到保密协议、竞业限制协议等法律文件的作用。妥善起草和签署这些法律文件固然重要，但是商业秘密的保护不能满足于这些文件。事前和事中的管理可能更为重要。

(一) 保护商业秘密不仅仅需要《保密协议》

我们坚信，作为行业领军企业的字节跳动，必然对其《保密协议》进行了周密的审查，并要求所有实习生签署。该协议无疑规定了违反保密义务或滥用商业秘密的行为，将导致赔偿字节跳动因此遭受的损失。据媒体报道，字节跳动已向实习生田某某提出高达 800 万元的赔偿要求。

如果字节跳动能够依据《保密协议》证明实习生的违约行为和侵犯商业秘密的事实，并证实其因代码攻击事件遭受了 800 万元的损失，且法院依法支持了字节跳动的诉求，判定实习生承担 800 万元的赔偿责任，那么接下来的问题在于：实习生是否具备支付这笔巨额赔偿的能力?作为一个尚未步入职场的独立民事主体，他是否有能力承担如此巨额的赔偿?即使其家庭为了避免子女受到“限高”的影响而不惜一切代价，他们是否能够承担这笔巨额赔偿?

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

因此，即便是 800 万元的赔偿判决，不论是否包含了字节跳动因研发延迟而产生的间接损失，对于字节跳动来说，这真的能够完全弥补其损失吗?

一份精心起草的《保密协议》不仅提供了保护商业秘密的行为准则，也是在商业秘密受到侵犯时寻求法律救济的最后保障。然而，商业秘密的风险防范远不止于一纸《保密协议》，它还应包括预防性的管理和过程中的控制措施。

(二) 事前的商业秘密风险管理

事前管理至少应涵盖人员审查和安全配置两个关键领域。

人员审查的核心在于对可能接触到企业商业机密的员工进行严格的背景调查，并在授予接触商业机密的权限时，综合考虑必要性和潜在风险。这一过程遵循“尚贤为本”的原则，旨在评估员工的历史合规性、经历等，以预测其可能对保密信息构成的侵犯、滥用或破坏风险。背景审查的焦点集中在三个关键点: (1)员工的信誉和合规历史，以防止有不良记录的员工接触企业的核心商业机密; (2)员工泄密风险的管理，避免那些配偶、近亲属或其他密切关系人从事竞争行业的员工接触企业的重要商业机密; (3)对于那些在加入企业前可能接触过竞争对手核心商业机密的员工，必须谨慎考虑其接触本企业商业机密的权限，以防信息泄露。

权限分配管理则是指根据实际需要，合理授予员工接触和处理商业机密的权限。这包括确定员工接触商业机密的范围和处理权限。权限分配的原则包括: (1)“按需分配”，即仅向因业务需要而必须接触商业机密的员工提供必要的、最小范围的权限; (2)“分权制衡”，即对于重要的、核心的商业机密，应避免将修改、批量导出等关键权限集中于单一个体。

在字节实习生事件中，商业秘密的事前管理值得讨论。首先，对于缺乏专业背景的实习生，是否应该直接授予其接触核心商业机密的权限，这一点值得考虑; 其次，对于实习生的工作内容，是否应该授予其直接修改核心代码的权限，同样需要慎重考虑; 最后，如果一个模型的修复成本高达 800 万，那么是否应该允许单个个体拥有篡改代码并发起攻击的权限，这反映出权限分配可能缺乏必要的制衡机制。

(三) 事中的商业秘密风险管理

事中的商业秘密风险管理涵盖保密制度的实施和人文管理两个方面。

保密制度的实施不仅包括《保密协议》中规定的保密行为，也包括企业制定的保密规章中员工行为守则。即使《保密协议》和保密规章制定得再完善，若不能在实际操作中得到有效执行，也不过是一纸空文。保密制度的实施应包括: (1)培训，以增强员工对商业秘密保护的意识; (2)考核，以核实员工保护商业秘密的能力; (3)执行，将保密制度规定的行为准则融入企

业日常管理，作为 OA 系统的一部分，甚至纳入 KPI 考核体系；以及(4)回顾，及时识别执行商业秘密保护中的难点和漏洞，并迅速采取措施加以弥补。

人文管理则是从关怀的角度出发，以减少商业秘密风险。如果说商业秘密培训是从认知层面增强意识，减少无意识泄露风险；那么人文关怀则是从动机层面减少故意侵犯商业秘密的可能性。“道之以德，齐之以礼，有耻且格”。在企业内部，避免恶性竞争，提倡共同发展，降低员工将企业视为“仇敌”的可能性，从而减少侵犯商业秘密的动机。

曾几何时，企业推崇狼性文化，将多元价值简化为单一的成功标准；良性的竞争被极端的社会达尔文主义所取代。如果企业价值和个人价值都变得功利化，所有人都陷入零和博弈的竞争中，那么规则的约束力将变得脆弱。如果企业和员工都能多些人性，少些狼性，那么员工对企业商业秘密的保护将更加自觉和自然。

正如字节跳动官方所解释，该研究生因对团队资源分配不满而篡改代码攻击训练模型。我们无法确切知道何种程度的分配不满会引发导致 800 万损失的攻击，究竟是实习生的行为过于极端，还是确实受到了重大打击。确实，实习生的二选一录用、末位淘汰等刚性制度，一方面激发了竞争，另一方面对于接触和掌握商业秘密的员工来说，无疑埋下了侵犯商业秘密的隐患。

二. 网络安全：不仅仅是技术问题

字节跳动实习生攻击训练模型事件，也凸显了网络安全的重要意义。

网络安全不仅仅是技术问题，也是管理问题，更是法律问题。维护网络系统的安全稳定，不仅仅靠技术能力的提升，通过等级保护，更是要依照《网络安全法》等法律要求，建立和执行网络安全管理制度。

对网络安全的管理包括事前、事中、事后三个环节。

(一) 网络安全的事前管理

在网络安全的事前管理中，对人的管理与权限分配至关重要，其重要性不亚于商业秘密的保护。

对人的管理的核心目标是防止不适宜的人员获得可能影响网络安全的操作权限。所谓“不适宜”的人员，指的是那些在合规记录、业务能力等方面存在问题的人员，包括那些有不良记录或缺乏必要操作能力的员工，以避免他们执行对网络安全构成重大影响的操作。

权限分配策略需遵循以下原则: (1)最小必要原则，即在业务需求的最小范围内授予权限，涵盖接触网络数据的敏感性、数据范围和网络操作权限等方面; (2)例外授权原则，即对于偶尔需要的高级别操作权限，应采取一事一议的方式处理，避免进行系统性的权限提升; (3)分权制衡原则，即将操作权限和数据库监控权限分离，确保重要操作需要双人复核。

与权限管理紧密相关的是系统隔离。只有通过有效的系统隔离，才能实现风险隔离，使权限分配具有实际意义。常见的系统隔离措施包括内网与外网的隔离、测试环境与生产环境的隔离，核心目的是将低风险环境与高风险环境有效分离，并分别进行授权管理。

我们尚不清楚字节跳动在网络安全事前管理方面的具体措施和效果。作为一家网络公司，我们相信其技术实力是雄厚的。字节官方声明，受到攻击的是训练模型，而生产环境未受影响，显示出其在两个系统间实现了有效的风险隔离。然而，如果一个实习生能够轻易篡改代码并攻击训练模型，造成高达 800 万的损失，这不得不让我们质疑是否给予实习生的权限过于宽泛。

(二) 网络安全的事中管理

网络安全的事中管理关键在于异常监测，即系统在检测到异常操作行为时，能够迅速向安全管理人员和部门主管发出警示，以便及时阻止可能危害网络安全的行为。异常操作的标准通常在 IT 安全管理规定中明确列出，并以代码形式嵌入网络安全管理系统，实现即时报警和处理。

典型的异常操作包括: (1)文件的批量下载、批量导出、批量处理; (2)安全配置的修改，尤其是降低安全级别的调整; (3)对系统核心安全数据或敏感数据的任何修改。

我们不清楚字节跳动的模型训练任务有多核心，其采取了什么样的安全措施。如果对该模型的任何攻击都应被视为异常操作，触发警报。若能迅速响应并制止这类攻击，就有可能显著降低损失。

(三) 网络安全的事后管理

网络安全的事后管理核心在于应急响应，即企业在遭遇网络安全事件时所采取的迅速恢复生产和降低损失的行动。恢复生产通常涉及切换至备份系统，以确保生产活动受到的影响最小化。而降低损失则通过数据恢复、保险理赔、舆论管理等多种手段来实现。例如，字节跳动在事件发生后迅速主动澄清事实，有效避免了对公司经营活动的疑虑，堪称舆论管理的典范。

网络安全的事后管理要求企业在网络安全事件发生前就制定详尽的安全预案，明确网络安全事件发生时的上报流程、分工职责以及具体的操作步骤。

在网络安全应急措施中，数据恢复至关重要，而数据恢复的前提是日常的备份和恢复验证工作。技术上，备份可分为全量备份和增量备份，无论采用哪种方式，都必须定期进行验证，以确保在网络安全事件发生后能够成功恢复。

目前尚不清楚字节跳动是否对其训练模型进行了备份。对于恢复成本高达 800 万的训练模型而言，如果平时就做好了安全备份，并在网络安全事件发生后能够有序地进行恢复，那么就可以最大程度地减少损失，并避免网络安全侵权者以“未采取补救措施”为由进行抗辩。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野