HZ BOOKS
华章IT

· 网络空间安全技术丛书 ·

企业安全建设指南

金融行业安全架构与技术实践

聂君 李燕 何扬军 编著

- 资深信安专家十余年实战经验的结晶，安全领域多位专家联袂推荐。
- 本书系统化介绍金融行业中企业信息安全的架构与技术实践，总结了作者在金融行业多年的信息安全实践经验，致力于解决金融企业信息安全“最后一公里”问题，内容丰富，实践性强。

机械工业出版社
China Machine Press

· 网络空间安全技术丛书 ·

企业安全建设指南

金融行业安全架构与技术实践

EFFECTIVE CYBERSECURITY PRACTICES

Architecture and Technology for Financial Institutions

聂君 李燕 何扬军 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

企业安全建设指南：金融行业安全架构与技术实践 / 聂君，李燕，何扬军编著 . —北京：机械工业出版社，2019.3（2019.6 重印）
（网络空间安全技术丛书）

ISBN 978-7-111-62203-1

I. 企… II. ①聂… ②李… ③何… III. 金融企业 – 信息安全 – 安全技术 – 指南 IV. F831-39

中国版本图书馆 CIP 数据核字（2019）第 046207 号

企业安全建设指南：金融行业安全架构与技术实践

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：吴　怡　　责任校对：李秋荣
印　　刷：中国电影出版社印刷厂　　版　　次：2019 年 6 月第 1 版第 4 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：27.75（含 0.5 印张插页）
书　　号：ISBN 978-7-111-62203-1　　定　　价：119.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　　读者信箱：hzit@hzbook.com

对本书的赞誉

我从事金融行业已有三十多年，经历了我国金融 IT 技术的发展和变化全过程。“安全可靠”是银行业的永久命题，它保障了银行信用的基础，全体技术人员时时刻刻为之付出了巨大的努力。互联网和云计算、大数据、人工智能等新技术的发展更加扁平化和立体化，对网络安全提出了新的全面要求。几位作者在银行和证券行业的安全技术领域不断探索实践，后生可畏。出版此书，殊为不易。

——徐连峰，原招商银行技术总监

本书是作者在金融行业多年从事安全工作的总结和归纳，对企业信息安全架构设计和安全技术实践的方方面面做了系统的梳理，实操性很强，干货满满！可以说，本书对金融行业信息安全从业人员和安全负责人都提供了一本行之有效的指南，可为案头常备工具书之一！

——陈建，平安集团首席安全官

信息安全是一项非常复杂的工程，既要有仰望星空的情怀，又要有脚踏实地的力行，这本书的作者们用自己的思考和实践很好地诠释了这一理念。几位作者都有十年以上金融信息安全从业经验，都是各企业的核心骨干，这次能够利用业余时间将这些经验编制成书，非常的难能可贵，自己有幸提前拜读，感悟良多，借此感谢。

——代留虎，招商银行总行安全管理室主管

建设完善的企业安全架构是一个非常艰难的过程，安全从业者的价值观和技术实战水平与企业安全的前途命运是紧密联系的，从安全本质出发，如何树立正确的安全价值观，处理好安全建设过程中的关系，把控安全趋势的发展，本书给予了我们启发和帮助。

——李吉慧，中国民生银行信息科技部安全规划中心副处长

本书是作者基于多年在金融行业网络安全技术管理岗位上的工作经验，针对金融企业的实际信息安全需求编撰的一部极具行业特色的著作。金融是离钱最近的行业，很自然就成为了网络罪犯们实施网络攻击的首要目标，金融企业必须要加强企业信息安全体系建设，才可能在与网络犯罪的对抗中力保业务不受损失。与此同时，金融企业的 IT 安全团队又往往只能有少量的人员编制，在这种情况下，如何进行企业的信息安全体系架构与团

队技术能力提升，往往是困扰团队领导的难题。而本书作者从安全架构出发首先讨论金融企业信息安全建设的一些策略性问题，然后深入到与金融企业业务紧密相关的安全技术实战，最后回到对金融行业安全趋势与安全从业者职业发展未来的分析上。全书内容深入浅出，语言流畅自然，特别推荐给金融行业网络安全从业者研读，可帮助其快速建立起对行业网络安全需求与安全策略的精准把握，以及对网络安全实战技术的全面了解。此外本书也适合其他行业网络安全从业者参考，毕竟金融行业在信息安全体系上的投入与建设理念可以作为其他行业的参照标杆。

——诸葛建伟，清华大学副研究员 / 蓝莲花战队联合创始人

在国内，具备甲方经验、有防御体系建设能力和实战经验的人才非常稀缺，随着网络安全的重要性日益提升，安全人才市场缺口凸显。本书出版恰逢其时，不仅系统介绍了企业信息安全建设的方方面面，同时作者以多年金融行业的安全实战为背景，给读者带来大量精彩案例，是网络安全从业人员手头不可缺少参考手册。

——董志强，腾讯安全云鼎实验室负责人

本书具有大安全的视野与格局，内容深入浅出，结合实践经验的分享，对大安全的各个方面进行了体系化的总结，理论不散、实践不浮，体现了作者多年的积累与思考，为各类金融企业提供了可参考借鉴的安全框架与实务手册。

——吴树鹏，火币集团首席安全官

任何技术的落地都需要和场景结合起来，安全技术尤其如此。金融行业是对安全需求非常高的，内部的应用场景和需求如何与现有的技术结合非常有参考价值。作者们总结了他们十几年在金融甲方的安全实战经验，让我读后受益匪浅，强烈推荐为金融行业提供安全产品和服务的乙方，以及准备去金融企业做甲方的安全技术人员阅读。

——方兴（flashsky），全知科技 CEO

金融行业的本质在经营风险，受到的监管合规管制也最严格。阅读本书，仿佛和作者们进行了一场酣畅淋漓的对话，又好像瞬间吸收了他们的功力，得以窥探金融领域安全实践的冰山一角。不论是大型互联网企业的安全管理者，还是初入行业的新人，本书都具有极大的参考意义，值得细细品读学习。

——赵弼政（职业欠钱），美团基础设施安全负责人

本书非常全面、系统、清晰地从多个维度介绍了企业信息安全建设的方方面面，对其中的主要场景的主要矛盾进行了深入浅出的剖析，既有适合安全管理者阅读的头脑激荡，

也有适合安全工程师阅读的实操经验分享，实战价值极高。本书极为适合安全从业者和安全爱好者阅读。

——方勇，腾讯云安全总监

金融行业一直是IT高度发展的一个领域，同时也是数据资产高度集中的一个行业。在这种背景下，相对其他行业，金融行业对于安全的重视程度普遍较高，安全技术和管理能力都更胜一筹。本书系统介绍了金融企业安全建设的方方面面，既有对抗技术，也有管理运营，对于其他行业的安全从业者也具有很好的指导价值。

——兜哥，百度安全基础架构安全负责人，AI安全三部曲的作者

金融行业对于安全的认识相对较早，同时重视程度也较高。作者们将多年在金融企业安全建设上的实践经验抽象成理念和可落地的方式、方法，并对金融行业常见的一些风险场景进行了全面深入的讲解，且有很多可直接落地的干货，对于安全规划、安全团队建设以及安全人员发展等痛点都有独到见解，相信金融行业安全从业者阅读本书后会受益匪浅。

——Feei（止介），美丽联合集团网络信息安全总监

本书是一本兼具安全架构和实战经验的信息安全专业书籍。本书的第一作者聂君先生在信息安全产业内工作多年，担任过知名金融机构的信息安全负责人，对甲方信息安全的需求，特别是金融行业信息安全的特点有着深厚的理解，在多年的信息安全管理工作中也积累了丰富的实战经验。本书的内容覆盖很广，从信息安全管理到最前沿的技术实战都有所涉猎，适合信息安全从业人员、金融行业IT从业人员等专业读者。

——萧德纲，启明星辰集团副总裁

本书是一本从甲方视角写的经验总结，读完后受益匪浅。今年上半年我们团队办了一场深度的Red Team闭门培训，本书第一作者聂君是学员中唯一一个甲方安全人员，当时他说他希望多吸收攻击者视角的手法，进而促进他们的安全工作。而读了此书，对我来说是大量吸收了防御者视角的经验，对我们以攻促防的安全建设思路来说是一次绝佳的学习机会。再次感谢。

——余弦，Joinsec Team & 慢雾科技联合创始人

许多信息安全的从业者受限于学习和工作的经历，没有机会洞悉信息安全的全貌，对于职业的规划和方向感到迷茫。许多企业的CEO、CTO和信息化负责人重视信息安全但

因缺少专业背景和知识，不知道企业安全岗位应该如何设置，安全建设应该如何开展。本书的几位作者在企业信息安全建设，尤其是金融企业安全建设方面有着丰富的实践经验，相信对于希望从事企业信息安全建设的朋友会有很大帮助。

——薛锋，微步在线 CEO

序　一

三年前认识聂君，初见时的场景仍记忆犹新。当时本人所在的企业急需引进一名在信息安全领域能够独当一面的专业人才，机缘巧合之下认识了聂君。几次接触发现，不仅他的知识和能力与岗位相匹配，更为重要的是我们彼此对很多事情的认识和看法非常契合，颇有相见恨晚之感。三顾茅庐之下，这位安全界大名鼎鼎的君哥终于被我感动，我也终为公司求得这一人才。

合作三年，感佩聂君做事的认真和用心，视角全面、思维成熟、敏于实践、勤于总结、乐于分享、广结人缘，若非如此，我想也断不会有此书的出版。

这几年，因工作的关系，我们在安全领域做了不小投入，下了不少功夫，对从事安全领域的甲乙方小伙伴们有了更多的了解，接触下来，真觉得十分有趣，也很欣赏。安全圈无论是国内外，颇有江湖侠客之风：英雄不问出处，尊重个性，崇尚技术，追求卓越；靠着先天之悟性加后天之勤奋，从业者可以一战成名，受众人尊重甚至追随。

当下，尤其是对金融机构而言，信息安全的重要性已经不需要再特别论证。或许各家企业起心动念起点不同，但无论是主动谋求长治久安，还是仅仅为形势环境所迫，无一例外都已经将信息安全作为一项重中之重的任务来抓。但真正要做好却着实不易。借此机会，我也从我的角度（甲方 IT 主管）对信息安全浅谈几点。

一、关于信息安全工作的定位：金融企业的商业价值是为客户提供金融服务，业务永远是其根本和主业，IT 的价值在于把技术做好，为公司提供先进的、安全的、有市场竞争力的 IT 平台和工具，服务好客户。因此 IT 万不可跳脱出来，就着技术论技术，甚至倒逼公司做投入。信息安全作为 IT 的一个细分领域，也同样必须统一到这个认识上。作为甲方的安全从业人员，必须基于公司的业务、发展阶段和内外部环境，综合统筹制定安全规划和实施路径，帮助企业达成商业目标，与业务的差别仅仅是分工不同、职责不同而已。

二、关于信息安全工作的重要性：经常听到这句话：信息安全做得好不好，首先取决于领导的重视程度。在我看来，这话对也不对。对的方面是：结果是否达成确实和领导有很大关系，如果公司不做投入，领导该承担的责任不承担，任谁都不可能做好这份工作；那为什么又说这话不对呢，因为领导不是神仙，在缺少信息支撑的情况下不可能做出预判和决策。安全人员自身要做好领域规划和布道宣传，有意识地提炼工作、向上管理。有时往往是因为自身能力的欠缺，这方面的工作做得不够，不同职场层次之间存在较大信息不对称，才造成了公司投入没有及时跟上。因此，无论是安全人员还是 IT 人员，这是需要时刻提醒自己和提升自己的地方。

三、关于信息安全工作的复杂性：信息安全领域包罗万象，涉及技术与管理、研发与

测试等全链条，从物理层到应用层，从机器到人都需要纳入到工作范畴里，从体系、规划、架构、管理与技术落地以及运营迭代形成闭环。这是一个复杂的系统工程，需要很强的系统性思维，持续不断的学习自驱力和卓越的执行力。

四、关于信息安全工作的横向协作：在IT团队内部，信息安全与研发、运维、测试等都需要密切的协作，但因为安全工作更多承担了制定规范、监控监督的职责，所以，在协作方面处理不好，容易出现工作冲突，损伤士气。甲方安全人员尤其需要对这一点有深刻的认识，在工作中能够客观看待事物和艺术的处理矛盾，积极主动、不忘初心的去达成目标，慢慢历练出专业感和职业感，当然要达到这一点是不容易的，但也是很重要的。

写序之前，仔细拜读了全书，书中所思所想皆发自作者肺腑，所行所感皆来自实践，内容全面翔实，可谓倾其所得、倾囊而出。对于上述几点看法，作者有着非常深刻的认识，其中观点我非常认同，此外，书中还在战术层面归纳总结了很多方法，具有很强的实操性，相信无论是甲方还是乙方的企业领导、CIO、安全主管，还是职场小白，都一定能从本书中得到启发，有所收获。

最后恭喜君哥儿女双全之外，集数年之功力，出版此书，可谓又喜得一子，可喜可贺。

许彦冰，安信证券信息技术中心总经理

2018年8月21日

序　二

自古以来，安全问题就是人类所要解决的最基本问题。小到每个人的安全，大到整个国家的安全，每个时代都无法回避这个问题。解决安全问题给人类生存和社会发展提供了基本保证。

自从互联网诞生以来，人类的生产力水平有了极大的提高，人们的生活随着互联网的出现变得越来越美好，但随之而来的安全问题，也以全新的面貌出现在我们面前，这带来了一系列新的挑战。

互联网、云计算、IoT、机器智能，这四项技术在短短二十年内的兴起，正在极大地改变整个世界。因为摩尔定律，计算和存储的成本每十八个月降为一半，也因此我们有能力将整个物理世界进行数字化，而数字化后的数据，通过互联网即时地传输回云端进行大规模计算的处理，从而诞生出了过去从来没有过的机器智能，而借助机器智能，我们真正拉开了一个时代的序幕。这个时代就像 19 世纪时人类进入电气时代一样，对我们的影响将无比深远。

我们所有安全从业者的责任，是很好地解决这个时代的安全问题，推动时代的进步与发展，而非让安全问题变成保守派与既得利益者的一种借口，阻碍社会的发展。先进生产力的出现，一开始往往是脆弱的、不完善的，也意味着肯定存在安全问题。但不能因安全问题的存在，因噎废食，彻底否定先进生产力。过于保守将极大地延缓人类进步的节奏，这与我们生活的环境息息相关。我想帮助先进生产力解决好安全问题，让新时代更快、更稳定地来临，正是我们安全从业者存在的意义。

在 19 世纪晚期，电气照明替代煤气照明的过程中就出现过种种争议，有人认为电气照明会带来不安全，让整个夜晚的城市照亮会方便罪犯在夜晚犯罪，甚至有报纸公开宣称照明是对神灵的亵渎。然而种种噪声终将消失在历史长河，但是这些争议却是工程师们设计一套稳定、安全系统的最佳磨刀石。出现安全问题必然意味着损失，甚至有牺牲，但需要整体保持乐观，不断总结经验就能向前走下去，终达彼岸。

安全问题是一个信任的问题。我们无从解决一个没有任何信任基础的安全问题，怀疑主义者如果怀疑一切，那么就失去了出发点。基本的信任就像一个世界中的原点，只有从原点出发，才有可能推导出一切。就像可信计算中的信任链传递，在最底层最基础的部分，一定有一个可信任的芯片，它是一切的基础。如果这个基础的信任假设不成立，那么构建的一切上层建筑将随之崩溃。

安全问题是一个研究对抗的科学。没有对抗，就没有威胁，也就没有安全问题。所谓安全，一定是有需要保护的一方，与形成威胁的一方。勿论这种威胁是来自于内部，还是来自于外部。人与人之间的关系，构成了现代社会，因此安全问题在很多时候，最终依旧要回归

到研究人与组织上面去。只有研究清楚了威胁一方的能力、动向，才能有效地调动我方的资源、部署。在对抗中，安全问题被不断解决。所以从宏观上看，我们要解决的安全问题，与军事上的很多思想有共通之处。而在互联网安全问题中，则衍生出了“威胁情报”这一分支。

安全问题是一个概率问题。安全事件往往是小概率事件，但在一个大规模环境下，小概率事件却往往又会变为常态。比如小行星撞击地球、地震、战争等灾害的破坏，很可能会影响到数据中心的数据安全，但这些极端的事件是一个小概率事件，不是每时每刻都在发生的，在设计系统时需要从全局考虑，更要平衡好对应的投入产出比。一个安全方案决定的是有限资源的分配，要把资源分配在概率最高、风险最大的问题上。但我们日常面临的种种安全问题往往不是那么极端，那么如何评估概率、分配资源，对安全架构师的能力提出了很高的要求。

安全是一门应用科学。从业十多年，我感受到安全这门学科并不像物理、数学一样有很多的基础理论需要去研究和探索。安全从对抗中来，最终还是要回到对抗中去，到底好不好，要看疗效。在不同时代、不同环境下也会衍生出不同的安全问题。因此如果说安全问题研究的是什么，我认为最终还是会回到研究人与人之间的关系。但在这个过程中，随着每个时代的不同，可以有很多不同的技术手段、工具应用到安全的对抗过程中，就是为了完成各自的安全目标。

安全工作者永远对新技术保持敏感、乐于接受先进生产力。无论是攻击还是防守，先进生产力都能带来很多新的视角、新的能力。比如新出现的机器智能，让我们对概率这一问题能够做到更加的心中有数，更加精细化地管理我们面临的一切。而对概率的计算越精准，就越能有效地分配资源，从而实现对抗中的优势，这不失为当前最需探索的一条新的道路。同样，区块链的出现，在可以预见的未来中，将成为极其重要的基础设施。在整个世界数字化的基础上，人类的一切行为有可能被全量记录在区块链的账本中，通过加密技术保证无法被篡改，这让我们有可能第一次真正解决数据共享中的信任问题。而信任的门槛被降低后，会像打开一个潘多拉的魔盒一样，改变人类生活的方方面面。这种对社会的推动与改变，正是安全工作者所应当追求的。

所有这些安全技术、安全问题的解决，都要立足脚下、放眼未来。作者们根据多年在金融企业的工作经验，写下了这本书。这本书对整个金融安全工作乃至各行各业的企业安全工作，都有着非常重要的指导意义。这是因为金融行业本身对安全的要求就非常高，是一切业务的基础，在严格的要求下才能形成高水平的队伍。另一方面金融本身研究的就是概率，对于安全问题会有着天然的敏感性，更勿论区块链技术最早就是在金融行业出现。也因此本书是从真正的一线中来并服务于一线的，书中既有理论思想指导，又有可落地的实操经验。

在本书中，我看到了作者们满满的诚意。将若干年的工作经验总结成文字是一件费时费力的事情，殊为不易，我们要感谢作者们的无私分享，而他们对于技术的谦卑心态值得我们所有人学习。

吴翰清，阿里云首席安全科学家

2018 年 8 月 26 日

序　三

得知君哥打算写这本有关安全运营的书时，满怀期待的同时也有一些疑虑。因为近几年网络安全相关的好书有不少，但多数是以安全技术为主，论述安全运营之道的非常鲜有。主要原因是安全技术领域纷繁驳杂，专注其中某项技术形成著作相对简单清晰。但安全运营之道不仅要融会贯通多项安全技术，还要根据业务系统的情况，把安全技术结合到日常安全运营工作中，并且在保障业务系统安全之余，还要考虑如何体现出安全运营工作的价值，这是一项需要长期坚持的浩大工程，其中还有很多讳莫难书的体会。所以，虽然知道君哥有多年的安全技术、安全管理的实战经验与积累，并且也从安全技术从业者转型为安全管理者，经历了安全运营工作中多个角色，有很多体会和心路历程，但繁忙工作和照顾家人之余，是否还能沉下心来梳理所学所感，把安全运营的宝贵经验都写出来，还是替君哥捏了一把汗。

所幸君哥和其他两位作者的积累和坚持，在我看到书本样稿时，不仅打消了之前的疑虑，更让我眼前一亮，这本积累几个作者心血的安全运营之道，不仅涉及当前安全运营相关常见的安全技术，而且能帮助和指导安全技术人员如何更好地运用技术提升安全工作。更包涵金融企业安全体系架构和建设的方向与内容，以及安全资产威胁管理等企业安全基础的重要关键点。更难能可贵的是，还结合作者从安全技术到安全运营管理的成长经历，提出了安全技术从业者可参考的“安全世界观”。更对企业的安全管理者和安全运营工作的负责人分享了很多宝贵的实战经验，让企业安全管理者和安全运营工作负责人，在面对企业领导、业务部门和用户希望安全工作是“不碍事不出事“的期望下，在安全投资难以衡量价值的前提下，如何围绕业务、协调好运维等各方面的关系，让安全运营工作顺利落地，如何让安全团队的技术价值显现，让搞安全的技术人员能够得到成就感。这些安全技术从业者和企业安全管理者思考多年也面临多年的“沉疴杂症”，给出了有实际参考意义的建议。也为当前部分金融企业的安全建设和从业人员点明了如何避免“为了安全而安全“的破局思路。对于日益多元化的需求和逐渐复杂的网络环境，让安全更应当回归实际，发挥安全工作的价值本质。

这本书对安全从业人员来说是一笔财富，亦是可让你随时翻阅、随时提供参考建议的良师益友。相信这本书能为金融企业构建有价值的安全体系提供有益的参考，同时能为致力于向 CSO（首席安全官）发展的安全人员，开启一些成长的思路。

这本书除了书籍文字之外，拜读之后还有不少感悟，安全工作门槛颇高，而黑白之间收益天差地别，但成功的安全人员离不开职业操守和情怀。安全人员的工作是解决风险，但也意味着随时暴露在风险和诱惑之中，当有捷径可走时，走还是不走？君哥和其他两位

作者分享所学，也正是在分享正面的“安全观”。

此外，“君哥的体历”公众号上破例发了一篇推广软文。推广“南俊苹果”，南俊是一名白帽黑客，在个人工作成长和妻子刚怀孕的人生美好时间，却因一场车祸，肩膀平面以下再没了知觉。但他没有因此颓丧，而是选择开一家名为“NJ的希望农场”的微店，通过销售老家农村有机苹果的微薄收入，以此承担照顾家庭的责任。求证南俊的事迹真实后，君哥为“南俊苹果”义气站台推广，还有安全圈同仁在朋友圈纷纷转发和支持，他和南俊都让我感受到了安全圈的这份温情、情怀与坚守，也正是安全圈满满义气的“人生观”的体现。

有幸作序之余，更多的是学习与感谢。安全工作充满挑战，道阻且长，但也机遇遍地，值得每一个从业者奋不顾身。在此寄愿安全圈的伙伴们始终都充满希望，始终有颗感恩的心，有颗持续让自己变得更好的心，永远坚持，永不放弃。

郭亮，北京数字观星科技有限公司

2018年8月28日

前　言

自从我从事信息安全职业以来，我一直在甲方从事企业安全建设工作。由于信息技术和安全技术日新月异地发展，我一直在学习之路上奔跑。看过很多书，听过很多演讲，其中大部分图书是零碎的技术点、工具使用和攻击过程演示，少数是属于理论性和学术性的教科书，很少有书籍介绍如何将安全技术更好地应用在不同规模、不同阶段的企业中，即企业安全最后一公里问题。在企业做安全、安全管理和安全技术，都需要通过安全实践去落地，并最终实现安全有效性的提升。

企业的安全负责人关注的重点是如何使企业的安全建设更加有效，以及如何落地，例如安全价值、安全如何保障业务、安全合规、安全总结汇报、安全考核、安全度量、资产管理等。企业安全建设的很多话题和讨论，看起来并不高大上，但却能够解决实际问题，给实际工作带来更大帮助，甚至很多属于“保命”的知识和技能。可是，安全实践这部分很有价值的内容却被市场选择性地忽略了。

企业安全建设中另一个重点是安全运营。企业负责人和 IT 部总经理经常会问：什么样的安全是安全的？我见过一些企业做安全的过程，部署了各种安全设备，设计了各种安全管理措施和流程，领导也很支持，安全预算和安全人员也都给足，结果还是出了问题，归根结底是安全有效性出了问题。设备部署了，异常告警规则做好了吗？告警正常吗？设备依赖的条件，比如镜像的流量一直正常吗？了解安全保护的业务吗？能看懂告警日志的人有吗……

要将安全性当作可用性来运营，安全才是有效的。目前制约安全运营发展的最大因素有两点：一是缺少特别好的商业化工具，能够结合企业内部的流程和人员，提高安全运营效率；二是一万个安全负责人心中有一万个安全运营思路，没有形成统一的安全运营标准。安全运营这部分很有价值的内容，很遗憾和安全实践一样，也被市场选择性地忽略了。

书本和市场提供不了这些知识和技能，我只能求教于同行。我的从业经历主要在银行和证券，因此每年我都会和行业同仁进行学习交流。除了金融业，我们也向互联网行业公司学习，从中确实获益良多。不同的行业、企业的规模、面临的风险威胁、企业文化和实际需求、安全投入等，其安全建设之路也风格迥异，但做得好的企业都侧重解决实际安全问题，日拱一卒，积极实践，因此愈发坚定我对安全实践和安全运营的探索。

利用工作之余的闲暇时间，我维护了“君哥的体历”公众号和“金融业企业安全建设实践”微信群，将我从业十余年的一些体验和经历分享出来，抛砖引玉，启发更多企业安全负责人的思考和分享讨论，并将有价值的内容沉淀在知识星球（公众号、微信群、知识星球联系方式见文末），为越来越多的人带来一些价值和帮助。

这种分享，我理解为另一种“开源”精神。代码和项目开源很常见，体验和经历开源不多见，尤其是比较体系化地将如何在企业做安全建设的思路和实践开源，需要静下心来归纳总结提炼，在平常繁重的工作任务和需要全身心投入陪伴两个娃的同时，要做好“企业安全建设”这个开源项目，难度和挑战更大。在这个过程中，有如西湖惬意的微风，也有如沙漠般的烈日当头。不忘初心，方得始终。初心易得，始终难守。幸好我遇到了两位志同道合的伙伴，我们彼此共同努力和坚持，克服了各种困难，才有此书的面世。

在某个年纪之前，你可以靠透支身体、小聪明和老天给你的运气，一直取巧地活着。然而到了某个年纪之后，真正能让你走远的是自律、积极和勤奋。人生最美好的莫过于各种经历和难忘的体验，过程虽然比较痛苦，结果都还比较好。如果大家和我一样，在企业做安全中遇到各种颇为“痛苦”的经历，过后你一定会感谢和怀念这份经历的。

本书结构

本书分两部分共 24 章，读者可以通过浏览目录进一步了解各章的内容。本书介绍了企业安全建设的方方面面，可以当作一本安全工作参考书，遇到问题时，也可以挑选任何所需要章节进行阅读。

第一部分“安全架构”，主要介绍了企业安全建设涉及的领域，金融行业安全建设的一些特点，重点安全管理领域如内控合规管理、外包安全管理等，对安全团队建设、安全培训、安全考核、安全认证、安全预算等进行了深入探讨，有助于读者从企业安全建设者的角度了解企业安全的视角和解决问题的思路。

第二部分“安全技术实战”，主要介绍企业安全建设中的一些安全技术应用实践，包括应用安全、内网安全、数据安全和业务安全等，对一些防护重点如邮件、活动目录、补丁管理、抗 DDoS 攻击等进行了深入探讨，对安全运营、应急响应和安全趋势以及从业者的未来做了一些开放式探讨。这些有助于企业安全负责人更好地掌握全局，顺势而为。附录中介绍了企业安全技能树等内容，还在持续更新中，有兴趣的读者可以和我们互动反馈。联系方式如下：

邮箱：niejun2002@gmail.com

GitHub：https://github.com/jun1010/secbuild

微信公众号：君哥的体历（jungedetili）

知识星球：金融企业安全建设实践

聂君致谢

感谢我的妻子，在最美丽的时候与我相遇，我的人生才充满了甜蜜快乐和多姿多彩。感谢她在我遭遇挫折和失败的时候默默支持着我，使我在迷茫和困惑的时候仍然能够鼓起勇气，看清方向。感谢生命中最可爱的两个宝贝，让我每一天都充满快乐和希望。

感谢我的父母，是他们养育了我。感谢我的父母和岳父岳母，帮忙照顾我的家庭，并一直支持我的事业，使我最终能有机会写下这些文字。

感谢我任职过的公司，给予我实践的土壤，使我能够有今天的积累。感谢工作中一直给予我帮助和鼓励的领导、同事和朋友，他们包括但不限于：吴云坤、周天虹、许彦冰、周智坚、高旭磊、贾俊刚、代留虎、徐恒、张靓、万雪林、何扬军、丁一琼、诸葛建伟、吴翰清、杨勇（Coolc）@腾讯、赵彦 @美团、董志强（killer）@腾讯、方小顿（剑心）、韦韬（Lenx）@百度、胡珀（Lakehu）@腾讯、吴树鹏 @火币网、王宇 @蚂蚁金服、赵弼政（职业欠钱）@美团、方勇 @腾讯、李吉慧 @民生银行、余弦 @慢雾、刘焱（兜哥）@百度、郭亮 @数字观星、顾孔希 @滴滴、方兴 @全知科技、Feei（止介）@美丽联合、shutgun@启明、薛锋 @微步在线、陈纯。

感谢许彦冰女士为本书作序，她是我非常敬佩的一位领导和学习楷模。

感谢吴怡编辑以及机械工业出版社的编辑、排版、设计等人员，他们非常专业和敬业。

最后感谢成长道路上给予我帮助的每一位朋友，感恩。

李燕致谢

在商业银行从事了多年的信息安全管理工作，几乎每天都在跟各种各样的报告打交道，监管报告、风险评估报告、安全检查报告、定期工作汇报……已经数不清楚写了多少份报告，感觉每天的工作，不是在写报告，就是在为了写报告而准备素材。但是在很多个失眠的夜晚，我不禁暗自思考：做了这么多项具体的工作，写了这么多份具体的报告，最终能留下的，到底还剩什么？报告本身已经完成了它短暂的使命，工作本身已经实现了它当时的价值。但是除了每天埋头完成这些来自各种不同渠道的任务以外，我可以给后面从事同类工作的小伙伴们留下些什么，能够积累、沉淀、传承些什么？一个人的力量是有限的，能直接管理和培养的团队也是有限的，如果能将个人的经历变成可以复制的经验，对于未来团队的培养，对于金融行业的信息安全工作，也许都可以是一个小小的贡献。

作为建立起两个商业银行信息安全团队的人，我深深了解信息安全人员的辛苦忙碌和酸甜苦辣，深深体会到信息安全人员的远大抱负和对现实的无奈，深深感动于信息安全人员的顽强坚守和价值追求。特别是金融行业，信息安全工作要求极高，信息安全人员压力极大，他们凭着极度的责任感和敬业精神，捍卫着金融企业科技的合规发展，保护着客户的资金和信息不被侵犯。我一直希望自己能做些什么，可以帮助后来的伙伴们拓展一些思路，少走一些弯路，加快一点步伐。把自己想过的、做过的、错过的，都分享出来，也许是个办法。

然而，事非经过不知难。信息安全永远没有最佳答案，只能动态平衡、不断调整。适合自己的就是最好的，但要找到适合的那个平衡点却是最难的。我们的书也给不出标准答案，只能给出一种思维、一套逻辑、一类方法和一些启迪，能保证的只是每一个字都来源于实际工作，都可以落地。如果本书能引起一些讨论，能像石头激起一些水花，或者能引发更多金融行业的同行们也将经验拿出来分享，那这件事情的意义就远远超出了文字本

身；如果我们的分享和总结，能带给读者们一点点启发和改变，我们的方法和工具能在企业中有一点点的应用和推广，那么我们的工夫就没有白费。

春节、清明、五一、端午、周末，已经记不清多少个假日在闭门码字，也记不清多少个晚上 11 ：00 以后在挑灯奋战。今天回首，很庆幸能够坚持不懈，很庆幸没有半途而废。工作是修行，写书是修行，人生是修行。修行，永远在路上。

感谢全力支持我的家人，这么多个不能陪伴你们的日日夜夜，你们仍鼎力支持，毫无怨言；感谢聂君，对我们运筹帷幄、严控进度，自己则信手拈来、才思泉涌；感谢何扬军，虽至今未曾谋面，但字里行间体现出的专业、自信，跃然纸上。以文会友，不亦快哉！

聂君说，等书出版以后，我们几个要好好庆祝一下。我说，额手相庆，不醉无归。不出书本身，而是为努力的自己，为自律的自己，为更好的自己。我们等这一天，等很久了，幸好，它来了。

何扬军致谢

某日在朋友圈忍不住吐槽一本翻译过来的书，有个朋友在下面回复问我啥时候也出一本书。当时没有多想 ，一来平时工作确实忙，二来过往从事了很多具体的技术工作，杂乱且不方便透露细节。

或许是深埋心底的文艺情结作怪，当 2017 年年底好友聂君说想合作写一本书时，我有点小兴奋并马上就答应了。心想凭着这些年工作经验积累以及曾经发表在外部或在内部分享的文章应该问题不大，实际上写起来却发现自己还是把事情想简单了。

安全领域所涉及的面非常广，每个点深究下去又是一个专业领域。为了对得起自己也对得起读者，在接下来的半年时间里，我的身心状态总是在工作和写书之间进行切换，很多个晚上、几乎每个周末都在公司加班码字，好多个深夜保安来关灯了才发现整层楼只有我还在公司。有些技术虽然基本原理大家都懂，但真正要讲清楚来龙去脉还要查阅大量资料，有一些技术细节还需要反复在实验环境中测试确认，确保不犯错。所以进度也是相对较慢。好在最终坚持了下来，感谢聂君、李燕的鼓励，感谢公司领导和同事的支持，更感谢家人背后默默的付出。在写书过程中，还参考了不少网络资料，并与一些同事、朋友进行了讨论，在此一并表示感谢，他们是（排名不分先后）：徐恒、李旬保、万雪林、黄炜程、王先伟、伍盛、魏强、王俊麟、许世杰、梁泉、李志强、万京平 @ 神华信息、谭德飞 @ 平安科技、黄启高 @ 微软、顾孔希 @ 滴滴出行、俞婷 @ 中兴通讯、钱文斌 @ 网联、唐勤 @ 广发证券、廖位明 @ 连连支付。

初次写书，由于能力和精力所限，难免有错漏之处，恳请大家指出其中的错误与不足之处，谢谢！