2018-2019年度金融科技安全分析报告

pwc 普华永道

CAICT 中国信通院

平安金融安全研究院
PingAn Academy of Financial Security

普华永道

普华永道中国内地、香港及澳门成员机构根据各地适用的法律协作运营。整体而言，员工总数超过17,000人，其中包括超过600名合伙人。在普华永道，我们的使命是解决重要问题以及建立社会信任。这是我们在提供专业服务及作出商业决定时的重中之重。

由于日益增加的网络安全威胁，高效的网络安全方案已经成为了企业必需的业务要求，普华永道网络安全和隐私保护服务团队在安全的策略和转型、隐私和客户网络安全保护、安全系统实施和操作、安全突发事件和威胁管理等四个重点领域帮助您从广义角度了解网络安全与隐私保护对企业经营起到的防御和促进作用。

中国信息通信研究院

中国信息通信研究院（以下简称“信通院”）始建于1957年，是工业和信息化部直属科研事业单位。多年来，信通院始终秉持“国家高端专业智库 产业创新发展平台”的发展定位和“厚德实学 兴业致远”的核心文化价值理念，在行业发展的重大战略、规划、政策、标准和测试认证等方面发挥了有力支撑作用，为我国通信业跨越式发展和信息技术产业创新壮大起到了重要推动作用。近年来，适应经济社会发展的新形势新要求，围绕国家“网络强国”和“制造强国”新战略，信通院着力加强研究创新，在强化电信业和互联网研究优势的同时，不断扩展研究领域、提升研究深度，在4G/5G、工业互联网、智能制造、移动互联网、物联网、车联网、未来网络、云计算、大数据、人工智能、虚拟现实/增强现实（VR/AR）、智能硬件、网络与网络安全等方面进行了深入研究与前瞻布局，在国家信息通信及信息化与工业化融合领域的战略和政策研究、技术创新、产业发展、安全保障等方面发挥了重要作用，有力支撑了互联网+、制造强国、宽带中国等重大战略与政策出台和各领域重要任务的实施。

平安金融安全研究院

由平安科技成立的业界首家综合性的金融安全研究及创新机构，以倡导和共建“科技+安全+生态”的科技创新及应用体系为核心，结合“政、产、学、研、金、介、用”生态体系，致力于构建“金融安全3.0”时代的安全生态圈，在金融关键信息基础设施安全、金融科技安全、金融业务安全风控三方持续创新实践，打造金融安全领先品牌，并努力推动和引领国家网信事业发展。

目录

P4 报告调查背景

P6 摘要

具体调研及分析报告
1. 交易安全领域
2. 数据安全领域
P10 3. 传统网络安全技术及安全管理领域

P17 展望

01 报告调查背景

本报告部分内容及数据来源于《2018-2019中国企业金融科技安全调查问卷》。问卷由信通院、平安金融安全研究院和普华永道共同发起，共回收80份样本，主要覆盖金融科技行业，参与者主要为安全架构师、安全咨询师及安全工程师，占比33.8%，其余包括首席执行官、首席信息官、网络安全官、IT部门负责人、业务部门主管等。

在被调研企业的企业业务性质及业务领域方面，本次调研涵盖巴塞尔银行监管委员会（BCBS）所定义的各类金融科技企业，包括支付结算、存贷款与资本众筹、投资管理、市场设施等，调研范围具有广泛的代表性；另外，被调研企业中也包括15%的传统金融企业。

按照巴塞尔银行监管委员会（BCBS）的分类方法，您所在的企业正在或即将展开的金融科技活动包括以下哪些?

选项	小计	百分比%
支付结算（支付结算包括手机和网络支付、电子货币以及区块链等）	29	36.3
存贷款与资本众筹（众筹、P2P网贷、电子货币、区块链等）	25	31.3
投资管理（机器人投资顾问、电子自动交易、智慧合同等）	23	28.8
市场设备（大数据、云计算、电子身份认证等）	32	40
其他类别	12	15
以上都没有	14	17.5

在被调研企业的企业规模上，本次调研涵盖由少于50人的金融科技初创企业，至企业规模达1500人以上的行业龙头企业，调研样本相对较为全面。

您的企业的规模是?

选项	小计	百分比%
少于50人	8	10
50-199人	11	13.8
200-499人	12	15
500-1500人	13	16.3
1500人以上	36	45

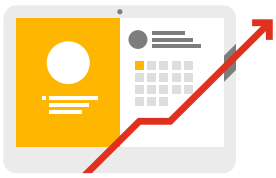
02 摘要

本报告是由普华永道、中国信息通信研究院、平安金融安全研究院共同撰写的《2018-2019年度金融科技安全分析报告》（或称“本报告”/“本次报告”），在平安金融安全研究院与绿盟合作的《2017年度金融科技安全分析报告》的基础上，由2017年度关注传统网络安全技术及安全管理领域对金融科技安全的影响，演变至在本次报告中关注金融科技安全中交易安全及数据安全领域的特点。这既反映了这一年多以来金融科技安全内容发展的趋势，也是我们持续关注业界最新发展并不断创新的表现。

金融科技的定义

2016年3月，全球金融治理的牵头机构—金融稳定理事会发布了《金融科技的描述与分析框架报告》（FSB, Fintech: Describing the Landscape and a Framework for Analysis），第一次在国际组织层面对金融科技做出了初步定义，即金融科技是指通过技术手段推动金融创新，形成对金融市场、机构及金融服务产生重大影响的业务模式、技术应用以及流程和产品（FSB，2016）。巴塞尔银行监管委员会将金融科技分为支付结算、存贷款与资本筹集、投资管理、市场设施四类（见表 1）。这四类业务在中国市场的发展规模、市场成熟度等方面存在差异，对中国现有金融体系的影响程度也有所不同。

表1：金融科技业务模式分类



支付结算

零售类支付
移动钱包
点对点汇款
数字货币

批发类支付
跨境支付
虚拟价值交换网络

存贷款与资本筹集

借贷平台
借贷型众筹
线上贷款平台
电子商务贷款
信用评分
贷款清收

股权融资
投资型众筹

投资管理

智能投顾
财务管理

电子交易
线上证券交易
线上货币交易

市场设施

跨行业通用服务
客户身份数字认证
多维数据归集处理

技术基础设施
分布式帐户
大数据
云计算

我国目前金融科技发展的关键简述

随着云计算、大数据、人工智能、区块链等信息技术在金融领域的逐渐推广及应用，金融科技正在以迅猛态势重塑金融行业生态，“无科技不金融”成为行业共识。中国金融科技产业发展迅速，涌现出一批在全球产业生态中占据重要地位的金融科技企业，以移动支付为代表的新金融应用更是成为中国的“国家名片”，被世界所熟知。

虽然，金融科技公司经历了互联网金融时代“颠覆者”的角色，一度迅猛增长，但近几年随着监管环境的变化和传统金融机构的回应，它们又改变策略，纷纷转而提供技术服务。这其中不乏传统大金融机构与互联网技术公司融合、合作，成立新的金融科技企业的案例（譬如中国银行+腾讯建立金融科技联合实验室，搭建总对总金融科技云平台等；农业银行+百度共建金融科技联合实验室，共建金融大脑以及客户画像、精准营销等）；在投融资领域，2018年，蚂蚁金服140亿美元C轮融资成为中国金融科技领域有史以来金额最大的一笔投融资事件，然而，大部分的金融科技公司重技术、轻场景，业务模式和技术同质化严重，应用场景不够清晰，导致发展面临瓶颈。大部分金融科技公司均认为在过去12个月内的融资难度加大，挑战主要来自监管、竞争及投资人审慎的态度。

问：贵公司在过去12个月融资遇到挑战的主要原因有哪些？

2019年8月，中国人民银行印发《金融科技（FinTech）发展规划（2019-2021年）》（以下简称《规划》），明确提出未来三年金融科技工作的指导思想、基本原则、发展目标、重点任务和保障措施。《规划》被视为政府及监管机构肯定金融科技发展及积极推动金融科技发展的信号。《规划》指出，金融科技是技术驱动的金融创新，到2021年，建立健全我国金融科技发展的“四梁八柱”，进一步增强金融业科技应用能力，实现金融与科技深度融合、协调发展，推动我国金融科技发展居于国际领先水平，实现金融科技应用先进可控、金融服务能力稳步增强、金融风控水平明显提高、金融监管效能持续提升、金融科技支撑不断完善、金融科技产业繁荣发展。

《规划》也明确了六方面重点任务。其中第四项重点任务专门提到“加强网络安全风险管控和金融信息保护”的要求；并且，《规划》全文共62次提到“安全”，可见监管对金融科技的网络安全保持了高度的关注。

金融科技的网络安全关键要素

我们认为，网络安全必须与每个行业的业务特点相结合，否则是没有价值的。随着金融科技产业的逐渐壮大与发展，传统网络安全技术、网络安全管理模式、金融业原有的网络安全技术与管理模式，也必将发生变革，衍生出与金融科技行业业务属性及特点相吻合的金融科技特有的网络安全技术与网络安全管理模式。

ISO在《ISO/IEC 27000: 2014》中定义了信息安全（Information security），包括三个主要方面：保密性（Confidentiality）、可用性（Availability）和完整性（Integrity）。然而，传统的信息安全定义不能完全适用于金融科技行业，无法反映金融科技行业的网络安全特点及趋势。在展开本分析报告之前，我们根据金融科技行业的业务特点、网络安全特点及趋势，先定义好金融科技网络安全的关键要素。

如下（图1）所示，左侧为传统的信息安全要素，右侧为金融科技的网络安全要素：

传统的信息安全要素

C I A

- 保密性 — Confidentiality
- 完整性 — Integrity
- 可用性 — Availability

金融科技的网络安全要素

T D C

- 交易安全 — Transaction Security
  - 安全身份认证
  - 交易智能风控
- 数据安全 — Data Security
  - 数据全生命周期管理
  - 个人信息保护
- 传统网络安全技术及安全管理 — Cyber Security
  - 安全服务
  - 安全技术工具

- 交易安全：

  针对交易安全领域，高达61%的被调研企业均使用“风控识别（反欺诈应用、风险动态监测、用户行为分析等）”技术来驱动金融业务，表明风控识别成为金融科技企业在交易安全领域的重点实施载体。

- 数据安全：

  在我们的调研分析中，数据安全在金融科技安全中被赋予了最多的关注。无论是已发生的安全事件比较集中在数据安全领域、未来计划增聘的网络安全专业人员主要集中在数据安全与个人保护领域，还是未来仍需加强的网络安全领域比例高达71%等，均体现出数据安全已经成为金融科技企业安全的关键领域及要素。

- 传统网络安全技术及安全管理：

  在前期普遍已投入资源部署传统网络安全技术及措施的背景下，传统网络安全技术及安全管理领域不存在影响金融科技企业总体安全性的决定因素。“抗DDoS”及“安全咨询服务（企业整体风险评估）”这两项传统网络安全技术及管理领域的服务，成为金融科技企业向外主要采购的网络安全服务（比例均达到47%）；而在传统网络安全技术领域，“Web应用防火墙（WAF）”成为金融科技企业向外主要采购的网络安全技术工具（比例达到71%）。金融科技企业普遍拥有大量的技术研发人员，精于研发符合自身业务特点及要求的应用系统及工具，但以上数字表明传统的安全技术工具仍然是属于“术业有专攻”的模式。即使是研发能力领先的金融科技企业，也仍然持续采购及使用外部专业公司的安全工具，未在安全工具自研领域投入更多的资源。

03 具体调研及分析报告

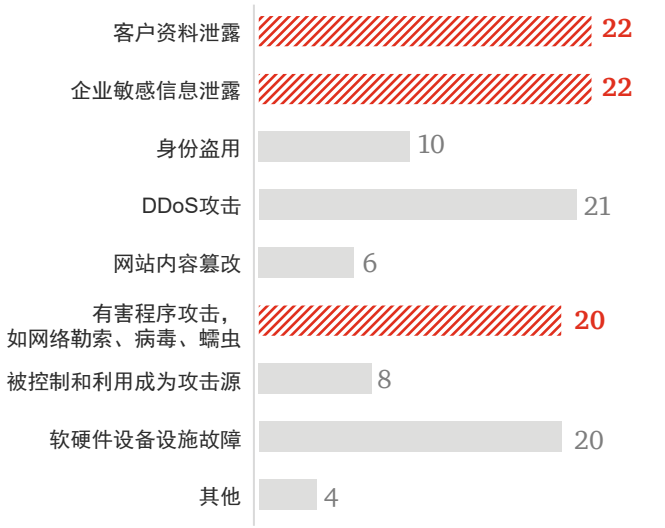
总体的调研及分析结果：

1. 在过去一年中，所有被调研企业均表示发生过不同类型的网络安全事件，其中，针对客户资料及企业重要业务数据的安全事件成为发生频率最高的安全事件类别，合计高达44%的比例（造成“客户资料泄露”约22%，以及“企业敏感信息泄露”约22%）；而“DDoS攻击”（占到21%的比例）及“有害程序攻击，如网络勒索、病毒、蠕虫”（占到20%的比例）则成为传统安全攻击类别的主要手段，特别是勒索病毒及蠕虫，延续自2017年以来WannaCry的余波，仍然在2018年至2019年上半年成为持续影响金融科技企业主要的网络安全风险。

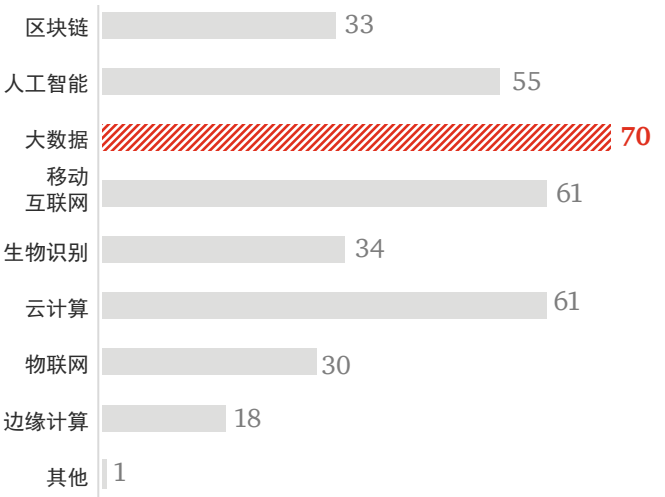
2. 40%的被调研金融科技企业以“私有云”作为其使用云计算服务的方式。

3. 金融科技企业的网络安全从业人员认为“大数据”（比例达70%）与他们的工作相关程度最高，可见大数据在业务风控、精准营销还是传统网络安全防御领域，均是金融科技网络安全的关键手段；“移动互联网”（比例为61%）及“云计算”（比例为61%）紧随其后，成为金融科技行业网络安全从业人员最关注及日常从事最多的工作领域。

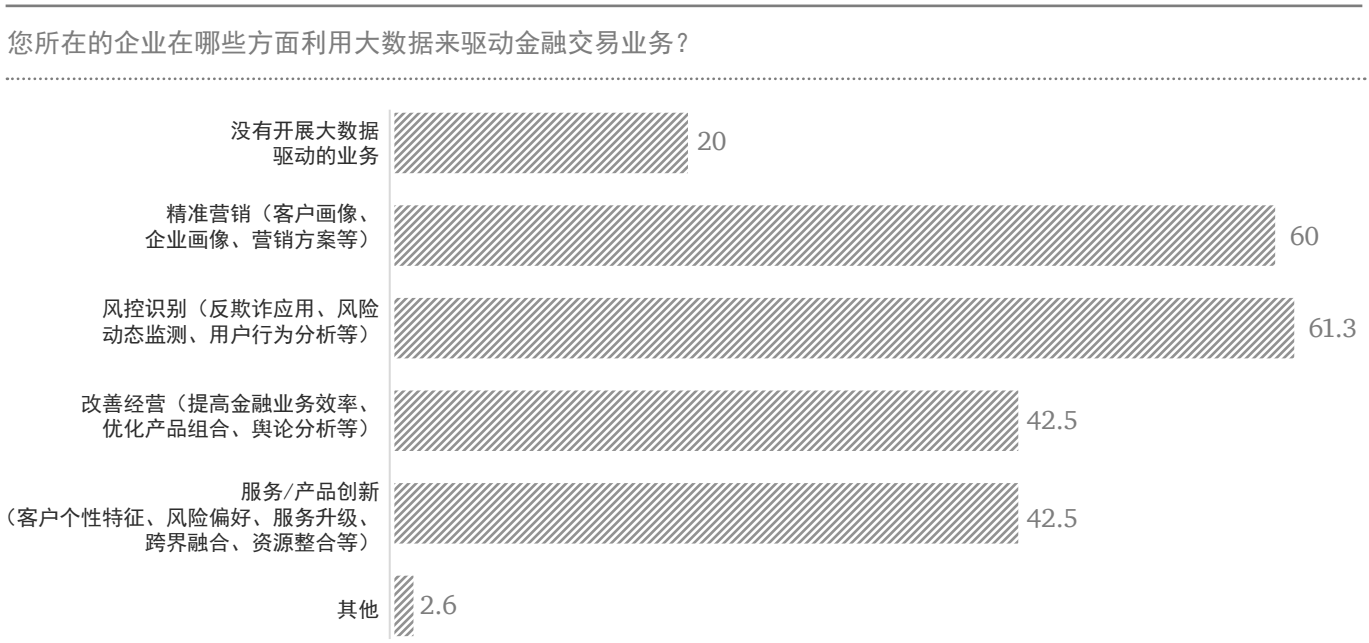
过去1年中，您的企业遭受过哪种类型的网络安全事件？



作为网络安全从业人员，您认为哪些技术或概念与您的工作息息相关？



4. 在另外一个调研及分析结果里，很好地响应了上一项分析结果，即只有20%的被调研企业没有利用大数据来驱动或者助力金融业务，其余的企业均在精准营销、风控识别、改善经营、服务/产品创新等一个或多个领域展开了大数据利用，具体如下：



5. 与大数据在用户画像、精准营销及风险防控等领域被集中应用不同，人工智能作为近一年半以来的热点应用，仍然未能出现能够集中体现其价值的核心领域，这表现在超过72%的被调研的金融科技企业逐步在其金融业务中使用人工智能技术，然而，有关使用却分散于各个领域：

我们认为这表明人工智能技术在金融科技领域依然面临“水土不服”的状态，仍然需要更多的时间才能实践出能够充分发挥人工智能优势的金融应用领域。

交易安全领域

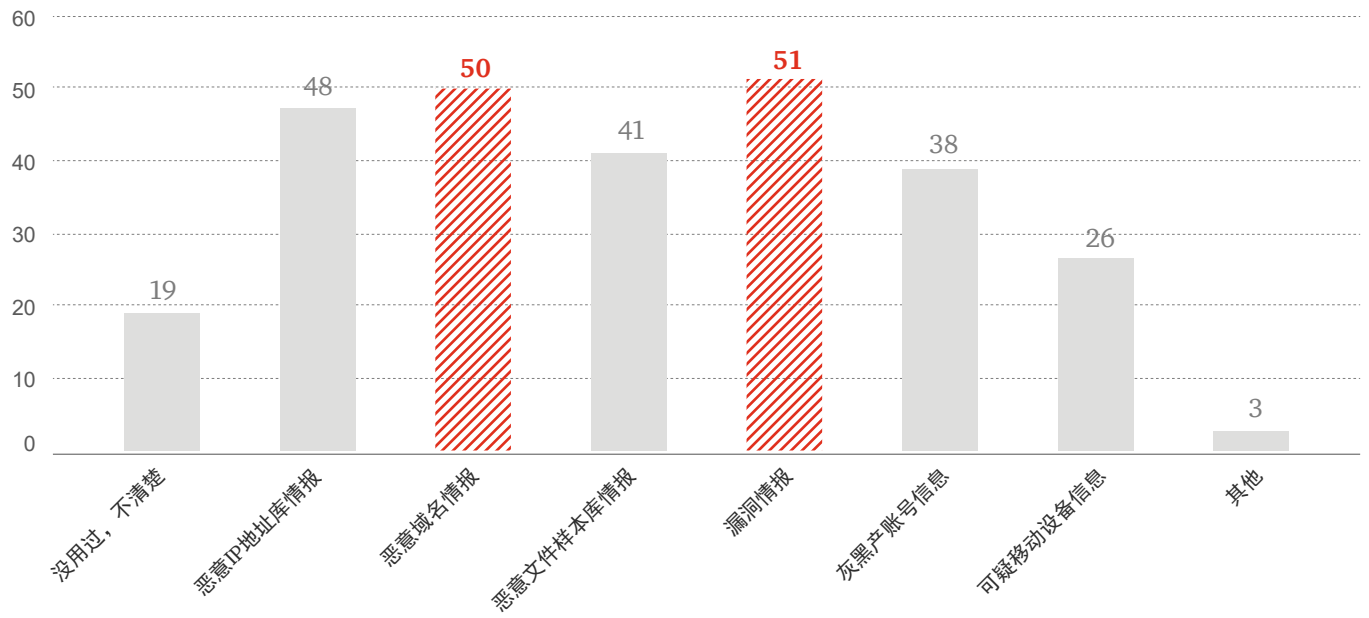
在金融科技企业向外采购的网络安全技术服务中，“威胁情报服务”达到35%的比例，这表明金融科技因线上交易的业务特点而普遍采取了对应身份认证及可疑交易风险的安全控制手段。针对威胁情报的具体内容，占比最大的仍然是传统网络安全风险领域的“漏洞情报”（51%），而针对交易安全领域的安全内容则涵盖了：

- 恶意域名情报（比例达50%）
- 恶意IP地址库情报(41%)
- 恶意文件样本库情报（41%）
- 灰黑产账号信息（38%）
- 可疑移动设备信息（26%）

有关的数据表明，在针对安全风险极高的身份验证领域，类似灰黑产账号信息及可疑移动设备信息等，金融科技企业仍然未普遍使用或者不愿意使用，其中的原因与另外一个调研结果相响应，即：

企业安全负责人认为威胁情报“有一定效果，但不知如何价值最大化”（占比达41%），同时，企业也在使用灰黑产账号信息及可疑移动设备信息等服务时，“感兴趣，但预算不够或不知道如何使用”（占比达33%）。可见，有关情报及服务如何更好地集成到金融科技的安全平台或者安全工具里，以便取得威胁关联分析和攻击溯源等良好的效果的课题，依然未在实践中得到良好的解决，我们认为系统异构及金融科技业务多样性是主要的原因；这也同时表明有关的服务及应用在未来时间段内将仍然拥有较为快速的增长需求及可能性。

结合您的经验，您认为目前威胁情报最具价值的内容是什么？



针对交易安全的攻击统计里，金融科技企业在过去一年半里面，普遍反映遭受到多种类型的业务安全攻击，几乎没有企业能够独善其身，具体包括：

- 交易安全（恶意贷款、积分套现、低价购买、市场营销活动薅羊毛等）（比例达33%）
- 账户安全（登录、注册、绑定关系找回）(33%)
- 系统级缺陷（二次打包、接口安全、应用层漏洞、数据存储）（33%）
- 支付安全（支付系统逻辑缺陷、支付行为可信、支付数据篡改、高并发资源竞争、信用卡套现/欺诈）（17%）
- 其他类型的攻击（21%）

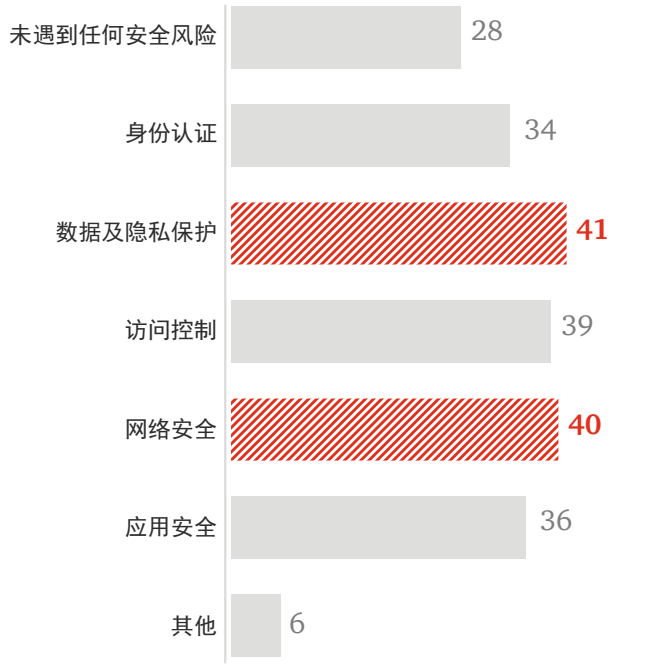
另外，针对数据/隐私安全的攻击也达到31%的比例，我们将在后续有关数据安全领域的分析中再详细阐述。

数据安全领域

72%的被调研企业已经有意识并且部署及使用数据脱敏的手段以保护客户及员工的个人信息，但是却仍然有37%的企业未与用户签署用户隐私协议以获取用户对企业使用个人信息的授权。这体现出金融科技企业虽然在具体的数据应用及保护实操层面已经采取了积极的措施，但在跟进个人信息保护的最新法律、法规要求方面存在一定的滞后性。

1. 41%的被调研企业均反映在使用云服务的过程中，曾遭遇数据及隐私保护方面的风险事件，这表明业务数据及个人信息数据在使用第三方存储及处理服务方面，仍然存在心理信任、实际合规符合性不足、透明度不足的问题。

在您的企业使用云计算服务过程中，曾遭遇过哪些安全风险点？



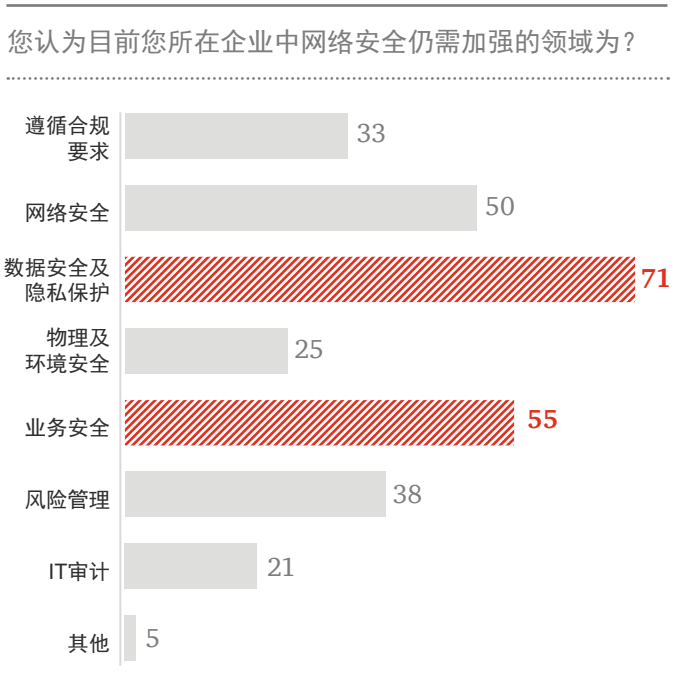
2. 国际上至少17个主要经济体国家及地区（包括中国），在过去两年中均制定或者实行与个人信息保护有关的法律、法规，导致收集大量个人信息并基于个人信息展开大量处理的金融科技企业，面临极大的合规压力与成本挑战。

   中国也由法律、法规及监管指引等层面均出台了一系列法律效力不等的个人信息保护及数据安全保护要求。

1996–至今持续更新	中国香港	The Personal Data (Privacy) Ordinance
2006	俄罗斯	Russian Federal Law on Personal Data
		The Data Localization Law
2016	印度尼西亚	Protection of Personal Data
2017	白俄罗斯	Informatisation and Protection
2017. 5	日本	Act on the Protection of Personal Information (APPI)
2017. 6	中国	网络安全法
2017. 10	新加坡	Personal Data Protection Act
	土耳其	Law on the Protection of Personal Data (LPPD)
2017. 12	波兰	Personal Data Protection Act (PDPA)
2018. 2	法国	Draft Data Protection Law
2018. 5	德国	Bundesdatenschutzgesetz, BDSG
	英国	Data Protection Act 2018
2018	欧盟	General Data Protection Regulation
	南非	Protection of Personal Information (POPI)
	巴西	General Personal Data Protection Act
2019	印度	Personal Data Protection Bill
2020. 1	美国	California Consumer Privacy Act (CCPA)

3. 71%的被调研企业表示，“数据安全及隐私保护”是企业目前及未来最需要加强的网络安全领域，这一项网络安全工作的受关注度及重要性远远超过其它网络安全工作领域。这一数字及比例表明，由于监管合规关注度增强、个人信息主体对个人信息保护意识度及要求的提升，金融科技企业正加大在此网络安全领域的投入。

4. 在应用新技术（主要指AI和大数据）的过程中，41%的被调研企业反映“大数据存储安全（数据加密等）”及31%的被调研企业反映“大数据使用和开放安全（访问控制、共享等）”是他们普遍遇到安全问题的领域。这显示AI技术的利用仍然处于初期阶段，而大数据的存储及共享使用已经给金融科技企业带来普遍的共性风险，需要金融科技企业在未来更加专注地投入资源及精力进行管理及应对，这也是大数据的风险特征及其使用目的所造成的。



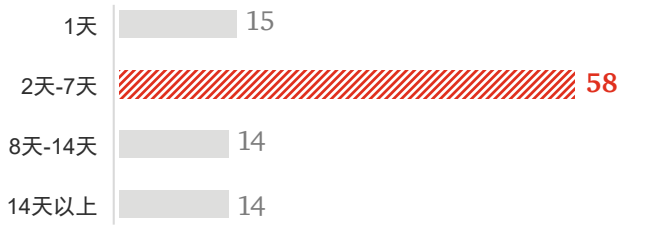
传统网络安全技术及安全管理领域

在过去1年中，所有被调研企业均表示发生过不同类型的网络安全事件，其中，

- 针对客户资料及企业重要业务数据的安全事件成为发生频率最高的安全事件类别，合计高达44%的比例（“客户资料泄露”约22%，以及“企业敏感信息泄露”约22%）
- “DDoS攻击”及“有害程序攻击，如网络勒索、病毒、蠕虫”则成为传统安全攻击类别的主要手段，占到20%左右的比例，特别是勒索病毒及蠕虫，延续自2017年以来WannaCry的余波，仍然在2018年至2019年上半年成为持续影响金融科技企业网络安全的主要风险。
- 另外值得关注的是，由于“软硬件设备设施故障”所造成的可用性中断的问题，比例竟然也达到20%，属于所有网络安全事件中发生频率较高的风险之一，我们认为这一比例表明金融科技企业在过往几年中，将网络安全注意力放在防范外部技术攻击的同时，可能忽略了传统网络安全风险中这一内部可用性风险。

1. 针对发生的网络安全事件，被调研企业中有51%可以在1天内侦测到有关事件，但仍然有高达49%的企业只能在2天-14天之后才能发现有关事件，其中，需要14天以上才能发现已发生的网络安全事件的企业达16%。这些数字及比例表明金融科技企业在安全自动运营（包括Security Operation Center，安全运营中心的建设及使用上）领域存在两极分化的现象，一方面是积极部署安全自动运营及检测机制与工具的金融科技企业，已经可以快速甚至实时地侦测到有害攻击及网络安全事件；另外一方面是缺乏有效监测及防入侵工具的金融科技企业群体。这与安全自动运营（包括SOC）的设备联接复杂、部署时间较长、投资较大有关。但长达14天以上的网络安全事件侦测时长，不得不引起广大金融科技企业网络安全管理层的关注。
2. 针对发现的网络安全技术漏洞，被调研企业中有57%需要花费2天-7天的时间完成漏洞修补，这一数据与金融科技企业普遍关注系统的主动稳定性及可用性有关，表明金融科技企业在更新系统补丁工作上的保守态度；特别地，仍然有13%的企业需要花费14天以上的时间完成漏洞修补，我们认为这是本次调研中发现的、金融科技企业最大的网络安全风险来源。

根据您企业漏洞管理现状，估算您的企业平均漏洞修补时间要多久？



3. 在金融科技企业向外采购的网络安全产品及服务中，“抗DDoS产品”及“抗DDoS服务”均排名靠前，分别为56%及47%，这与前面我们了解到金融科技企业普遍受到“DDoS攻击”（比例21%）的结论表明金融科技企业在线上业务载体普遍受到流量攻击的同时，也在积极寻求外部专业技术及服务协助。

4. 在普华永道《第21期全球CEO调研中国报告》中，51%的金融业受访CEO均计划在未来12个月内招聘更多员工；而在我们本次的调研中，只有6%的被调研金融企业表示在未来年度会减少网络安全人员编制，换句话说，94%的企业将在来年持续加大网络安全投入，包括聘请更多的网络安全专业人员，其中，计划增聘10位网络安全专业人员的企业达到7%的比例。这些数字及比例表明网络安全人才市场仍然处于卖方市场，特别是专业的金融科技专业网络安全人才仍然处于供不应求的状态。

5. 在网络安全的预算投入方面，35%的被调研企业计划在来年增加20%以内的网络安全预算，10%的被调研企业拟增加20%-50%的网络安全预算。这些数字及比例表明网络安全对金融科技企业业务的重要性正在不断增强，也表明企业管理层对网络安全的认可及关注正在不断增加。

6. 在传统网络安全的基础保障管理领域，超过一半（58%）的金融科技企业部署及实施了“安全开发生命周期（S-SDLC）管理体系”。这是一项比较耗资源的网络安全防护措施，但能够极大地将网络安全风险往“事前”、“业务前端”转移，相对来说可以更有效地防止网络安全风险产生实质性的影响，可见金融科技企业已经普遍认识到它能够带来的效果，也愿意投入更多地资源在这一耗费较多人力资源的领域。

参考资料

- 中国人民银行《金融科技（FinTech）发展规划（2019-2021年）》
- 中国信通院《2019年中国金融科技生态白皮书》
- 普华永道《第21期全球CEO调研中国报告》
- 普华永道《2018年中国金融科技调查报告》
- FSB, Fintech: Describing the Landscape and a Framework for Analysis
- ISO《ISO/IEC 27000:2014 Information technology - Security techniques - Information security management systems — Overview and vocabulary》

展望

没有百分之百的网络安全工作，也没有百分之百的网络安全保障手段及解决方案，网络安全工作是一项长期投入并需要各业务条线及各职能部门共同配合及推进的工作。

数据安全持续成为金融科技行业的工作重点—在这一项长期的工作里，网络安全的内涵及其在每个行业的应用内容，均在不断地发生变化。正如我们在开篇所阐述的，自上一期金融科技安全分析报告至本次分析报告期间，金融科技的网络安全趋势及具体内容已经发生了较大的变化，譬如在2018年至2019上半年期间，无论是网络安全事件比较集中发生在数据安全领域、或者是企业拟向数据安全领域投入较多的资源等，均体现出数据安全正成为监管高度关注、行业风险集中的领域。我们预计数据安全在未来两年内持续成为金融科技行业、金融行业的网络安全工作重点，特别是在金融科技这一强监管行业，伴随《个人信息保护法》及《数据安全法》两部重要法律列入立法规划，切合时代需求和中国国情的数据监管法规必将进一步使得数据安全成为金融科技行业的工作重点。金融科技企业内部的安全团队将在未来两年均划分成为独立的网络安全及数据安全部门/团队。

数据得到更广泛、真正的利用—截止目前，中国金融科技行业甚至互联网行业在数据利用上，或者说真正将数据用好的领域，依然局限在用户画像、精准营销及风险防控上，其它利用领域的应用水平仍然远远不及；数据应用场景也十分局限，行业仍然未能发掘出更多数据应用领域。未来两年，随着过往数据利用的经验积累，我们预计行业将有可能真正用好数据，使得数据真正发挥“石油”的作用。根据目前行业内的数据应用水平，谈数据应用、数据是“石油”等，仍然为时过早。并且，由行业数据使用的安全成熟度来看，数据使用安全合规及数据使用技术安全（如脱敏等）仍然远远落后于业务需求的发展，所以，行业目前阶段的数据使用成熟度、数据安全成熟度仍然较低。

数据的融合、数据定价及数据资产化出现行业标准并得到监管认可—数据的充分融合才能提升其价值并进一步带动金融科技及互联网金融的生产力，数据资产化的标准将首先在金融行业或者互联网行业出现，并有可能在行业允许实践的基础上，在未来三年内得到金融监管机构或者其它监管机构的认可。

金融科技的创新应用—伴随大数据、云计算、区块链/虚拟货币、虚拟银行、无人银行、人工智能、RegTech等众多金融科技应用基础技术及应用场景的出现，金融科技在未来两年将持续向传统金融领域渗透，出现更多的创新应用。我们无法判定哪个基础技术及应用将为金融行业带来颠覆性的改变，区块链及人工智能作为基础技术，存在更大的未来想象空间及可能。我们一直认为网络安全与业务结合才有价值，所以，未来两年除数据安全以外，网络安全也将在区块链及人工智能领域（特别是人工智能隐私安全领域）持续得到行业关注及资源投入。