

A digital faucet dripping data. The faucet is a metallic, futuristic-looking tap with a handle. From the spout, a stream of glowing blue and white binary code (0s and 1s) flows downwards. The background is a dark blue gradient with a repeating pattern of binary code, creating a sense of depth and digital space.

在 数字时代的 直面 数据泄露事件



今社会，不完善的安全制度、员工失误或渎职、技术缺陷和狡猾的黑客等常见问题，可能导致严重的数据泄露事件。企业必须采取适当的政策和程序来应对这些威胁。¹

什么是数据泄露？

对数据泄露最常见的描述是未经授权使用或披露未经编辑或加密的个人信息（数据），对特定个人或群体造成（声誉、财务）损害的重大风险。²

数据泄露的主要原因

研究表明，美国企业面临的最大的网络安全风险是员工疏忽大意。³ 超过40%的数据泄露是由于员工的疏忽造成的。⁴ 员工可能在网络钓鱼、⁵ 鲸鱼型犯罪⁶ 或电话钓鱼攻击期间自愿向攻击者提供机密信息。⁷ 员工还可能下载未经授权的软件和恶意软件，导致病毒⁸ 或蠕虫，⁹ 使攻击者能访问专用网络及其设备。这就是为什么在入职流程中定期（至少一年一次）对员工进行安全培训应为继续雇佣的必要条件。

数据泄露也是由于缺乏安全控制措施和技术缺陷造成的。¹⁰ 在技术投入使用之前，通过良好的变更管理计划来测试技术，可以防范实施有缺陷、不安全的技术。补丁管理同样重要；通常对技术安装补丁可以修复漏洞、防范黑客入侵并防止数据泄露。¹¹ 此外，变更管理计划提供了一项流程，可以对员工所做的所有系统变更进行跟踪、审计、控制、识别和批准。¹²

此外，应在合并和收购过程中着重审查系统和控制措施，否则会导致数据泄露。

此外，供应商监督也同样重要。与缺乏控制措施且不符合监管要求的供应商签订服务合同，几乎总会带来灾难，也是造成重大数据泄露的原因。¹³

监管要求：数据泄露通知法案

世界上大多数国家的监管要求，都要求企业报告数据泄露事件。¹⁴

政策和程序同样是信息安全 管理的重要组成部分

2018年5月,《通用数据保护条例》(GDPR)正式生效。¹⁵ GDPR 管辖欧盟¹⁶和欧洲经济区¹⁷居民个人数据¹⁸的使用和披露。GDPR 规定控制人必须在发现数据泄露事件后72小时内向相关监管机构报告。¹⁹ GDPR 规定罚款金额最低为1,000万欧元或全球总收入的2%,最高可达2,000万欧元或全球总收入的4%。²⁰

目前,美国所有州都有数据泄露通知法规。最近两个颁布数据泄露法规的州是2018年的阿拉巴马州²¹和南达科他州²²。这意味着,如果企业遇到的泄露事件影响了美国消费者,不仅必须遵守适用的联邦法律(如《健康信息流通与责任法案》[HIPAA]²³和《金融服务现代化法案》[Gramm-Leach-Bliley Act]²⁴),还必须遵守适用的州泄露通知法规。HIPAA 要求发现后在合理时间内报告影响超过500人的泄露事件。²⁵许多州的泄露通知法规的报告要求并不明确。²⁶

2018年底,北卡罗莱纳州检察长讨论了对《州泄露通知法案》的拟议修正案,从模糊的通知期限修改为发现之日起15天的报告期限。²⁷2018年,纽约颁布了一项网络安全法²⁸,专门适用于受纽约州金融服务局监管的企业。纽约州的这项法律将于2020年生效,要求该法规管辖的企业在发现泄露事件后72小时内报告。²⁹华盛顿州最近修订了《数据泄露通知法》,将个人识别信息的定义扩大到包括个人健康信息和生物特征数据。华盛顿的报告要求时限最长,为发现后45天内。³⁰目前,只有少数几个州正在修改数据泄露法律或制定额外的安全或隐私法规。

数据泄露预防策略

企业可以采取一些措施来防止数据泄露。这些措施包括但不限于实施供应链管理、隐私信息安全程序和经过检验的事件管理计划。

许多法规都要求企业拥有供应商管理程序(如GDPR、³¹ HIPAA、³² 萨班斯-奥克斯利法案、³³ 《银行保密法》³⁴)。此外,管理供应商关系还有许多理由,包括供应商合规、适当测量第三方供应商对企业信息安全标准带来的风险和让供应商证明其能够满足合同中的责任和保密要求。³⁵

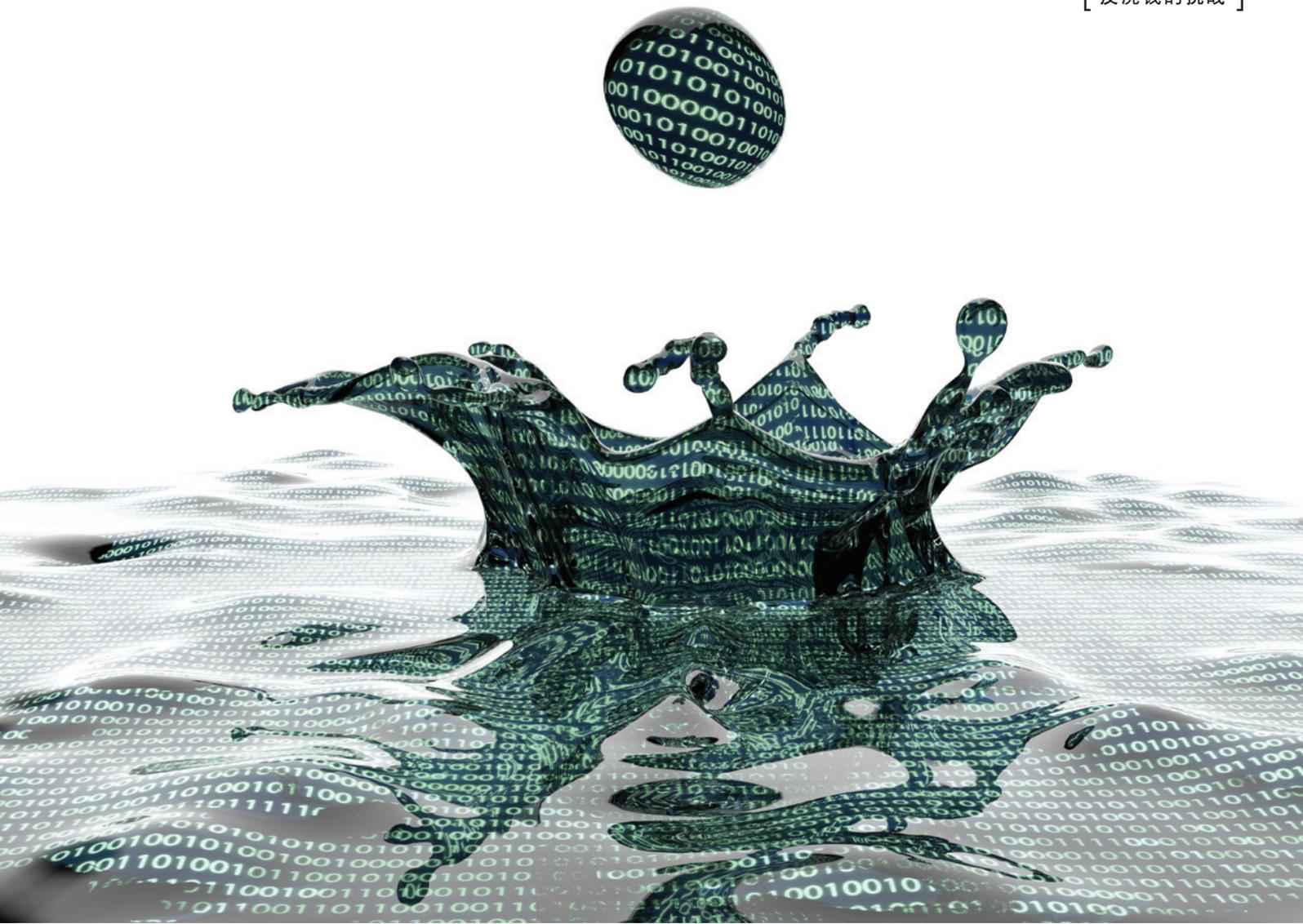
政策和程序同样是信息安全管理的重要组成部分。良好的信息安全程序可以降低网络攻击的风险,并能在攻击发生时及时有效地侦查和响应。³⁶ 应向员工沟通信息安全程序,使员工了解程序并理解政策。良好的信息安全政策应符合以下三项主要要求:

- 保密: 根据个人隐私权及合同或通知另行规定的方式存储信息。
- 诚信: 更新信息和程序以保持准确。
- 可用性: 授权用户能够访问信息和资源。³⁷

如前所述,员工有意或无意的原因造成了约40%的数据泄露。³⁸ 为了防止这种特定的数据泄露源,企业的最佳策略之一是教育不知情的用户。员工培训计划应针对现有和新员工、承包商以及短期供应商。企业应该使用多种交付方法进行培训(例如,现场、网络、桌面演练)。培训应适合个人的角色和访问级别。³⁹ 垃圾邮件过滤技术有时可以防止网络钓鱼,但这往往是不够的。还应告知员工点击可疑链接和从未知发件人下载附件的危险性。⁴⁰

几乎所有涉及未经授权访问或数据泄露的预防措施都包括加密,少数司法辖区除外⁴¹(如加利福尼亚州⁴²)。加密的定义是使用数学算法将纯文本转换为密文的过程。需要通过密钥来逆转这一过程并将数据还原为纯文本。⁴³ 加密可用于保护通过计算机网络传输的数据或位于USB、硬盘、USB驱动器、电话和存储设备上的静止数据。如果加密驱动器有未经授权用户访问或被窃取,加密数据对未经授权用户来说基本上无用、不可用,因为如果没有加密密钥,用户无法将数据转换回纯文本。⁴⁴

为了向用户提供对敏感系统的不受限制的权限,企业可以实现基于角色的访问(RBAC),以便分离员工的职责,提供员工访问活动的审计线索,并只授予用户执行工作所需的访问权限。限制用户可以访问的数据量限制了用户可能导致的数据泄露量。⁴⁵



除了 RBAC，身份验证也是防范网络攻击的一种良好安全实践。身份验证是指确保记录用户确实是授权或预期接收方或发送方。身份验证是机构对请求访问记录的个人或实体的身份建立适当程度的信任的过程。身份验证通过各种审查方法建立，这些方法也称为“身份验证因素”。“当用户具备身份验证因素时，就在一定程度上可确信访问用户就是它声称的个人或实体。⁴⁶

入侵侦查系统是另一种有效的安全机制。入侵侦查是对计算机系统或网络中可能发生的事件进行分析和监控的过程，以发现潜在事件的迹象。入侵侦查系统是执行入侵侦查流程的自动化软件。入侵防御系统也是一种能够防范事件的侦查系统软件。⁴⁷

另一种安全工具是实施防火墙。防火墙由一组相关程序组成，这些程序可防止入侵者访问专用网络上的数据。防火墙必须正确安装才能有效运行。防火墙可阻止外部设备向正在运行的工作站发起通信会话。在工作站上运行的防火墙和应用程序软件可防止与外部设备的意外出站连接。⁴⁸ 远程工作的员工应该使用虚拟公共网络（VPN）。⁴⁹ VPN 是一种使用公共电信基础设施传输数据的安全专用网络。VPN 使用身份验证和端到端加密⁵⁰来维护隐私和安全。⁵¹

最后，网络攻击的另一个重要防御手段是事件管理计划。当企业发现泄露事件时，他们如何处理、阻止或减轻事件将在很大程度上决定企业所受的罚金、罚款和声誉损害。根据经验，企业应该对其事件管理计划进行测试或接受独立评估。⁵² 制定事件管理计划，包括以下步骤：⁵³

- 指派能对事件做出适当反应的团队，确保周边（网络和物理位置）的安全，并防止进一步泄漏。
- 指派能识别事件来源和保存证据的法医团队（内部或外部）。
- 指派律师以评估法律、隐私和安全后果，以及报告要求。

- 指派公共关系小组来传播有关该事件的信息。

虽然这些方法并不能确保预防和管理事件万无一失，但根据国家和国际标准，它们通常是良好实践。⁵⁴

最近的大量数据泄露事件：案例分析

芝加哥公立学校（CPS）的一名员工复制并删除了包含敏感信息的数据库，之后被解雇。被盗信息包括 CPS 员工、志愿者等信息。⁵⁵ 2007 年，Certegey Check Services Inc. 的一名员工将约 220 万人的个人信息卖给了身份不明的数据经纪公司。然后经纪公司把这些信息卖给了几家营销公司。⁵⁶ 这些类型的攻击突显了 RBAC、审计线索和适当的离职流程（包括终止员工访问）的重要性。

2016 年，Snapchat 遭遇了鲸鱼型攻击造成的数据泄露。这名攻击者欺骗了一名员工，假装是 Snapchat 首席执行官 Evan Spiegel，获得了约 700 名现任和前任雇主的薪资记录。⁵⁷ Snapchat 的泄露事件表明，缺乏用户 / 员工意识和培训可能会对企业产生严重的影响。

2017 年 Equifax 的数据泄露是由其网站上的应用程序漏洞造成的。这次泄露泄露了超过 1.479 亿消费者的个人信息（社会保障号、生日、地址，在某些情况下，还有驾照编号）。⁵⁸ 2016 年，Equifax 曾因安全漏洞被起诉，当时该公司网站遭到攻击，导致 430,000 人的个人信息（姓名、社会保障号等）泄露。⁵⁹ 2013 年 4 月至 2014 年 1 月，Equifax 再次遭受攻击，攻击者使用足够的个人信息获取信用报告，以满足 Equifax 的身

根据经验，企业应该对其事件管理计划进行测试或接受独立评估

验证流程。⁶⁰ 很明显，多年来 Equifax 的安全系统一直问题不断，在四年多的时间里都没有纠正这个问题。

2018 年末，万豪发现其子公司喜达屋的预订系统在 2014 年启用后出现数据泄露。攻击者获得了大约 5 亿人的电子邮件、姓名、地址、护照号码，可能还有付款卡信息。尽管万豪酒店拥有网络保险，但公司股价在事件发生后下跌了 5%。万豪的网络入侵事件，说明了并购尽职调查的必要性。⁶¹

2013 年，Target 公司发现攻击者首先入侵了 Target 和 Target 的供暖和通风系统供应商之间的“数据连接”，意图入侵其支付系统。⁶² 2014 年 Target 公司的目标利润下降了 46%。⁶³ 2018 年，Target 公司在全美范围内就 2013 年的黑客入侵事件支付了 1,800 万美元的和解金。⁶⁴ Target 公司的泄露事件说明了供应商尽职调查的重要性。

结语

对许多企业来说，数据泄露可能意味着监管部门的罚款和制裁、声誉受损以及对消费者的额外责任。企业必须制定适当的政策和程序，防范技术故障，打击网络犯罪，对供应商进行尽职调查，并对员工进行入职培训和意识培训。省掉这些措施中任何一项所带来的风险，其代价远高于实施适当的控制措施的成本。⁶⁵ 

Victorianne C. Musonza 律师，CAMS，律师、隐私与安全顾问，
美国纽约州纽约市，Attorney@maxwelllegal.com

¹ “Creating a cyber security policy for your business”（为企业制定网络安全策略），*business.gov.au*，2018 年 7 月 27 日，<https://www.business.gov.au/risk-management/cyber-security/creating-a-cyber-security-policy-for-your-business>

² “国家数据泄露通知法律”（State Data Breach Notification Laws），*Foley & Lardner LLP*，2019 年 1 月 28 日，<https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws>

³ Carmen Reinicke，“The biggest cybersecurity risk to US businesses is employee negligence, study says”（研究称，美国企业面临的最大的网络安全风险是员工疏忽大意），*CNBC*，2018 年 6 月 21 日，<https://www.cnn.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html>

⁴ Mark Kaelin，“More than 40% of reported security breaches are caused by employee negligence”（超过 40% 的安全漏洞报告由员工疏忽造成），*TechRepublic*，2018 年 7 月 23 日，<https://www.techrepublic.com/article/over-40-of-reported-security-breaches-are-caused-by-employee-negligence/>

⁵ “Definition: Phishing”（定义：网络钓鱼），*国际信息系统审计协会（ISACA）*，<https://www.isaca.org/Pages/Glossary.aspx?tid=1682&char=P>

⁶ “Whale Phishing”（鲸鱼型网络钓鱼），*Trend Micro*，<https://www.trendmicro.com/vinfo/us/security/definition/whale-phishing>

- ⁷ “Vishing” (电话钓鱼), *Techopedia*, <https://www.techopedia.com/definition/4159/vishing>
- ⁸ “Definition: Virus” (定义: 病毒), *ISACA*, <https://www.isaca.org/Pages/Glossary.aspx?tid=1971&char=V>
- ⁹ “Definition: Worm” (定义: 蠕虫), *ISACA*, <https://www.isaca.org/Pages/Glossary.aspx?tid=1997&char=W>
- ¹⁰ “常见的网络攻击: 减少影响” (Common Cyber Attacks: Reducing the Impact), *国家信息保障技术管理局*, 第 3 页, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf
- ¹¹ 同上。
- ¹² Ed Tittle 等, *CISSP(r) Certified Information Systems Security Professional Study Guide (CISSP (r) 认证信息系统安全专家学习指南第 2 版)*, 2004 年, 第 41 页。
- ¹³ “Best Practices in Cyber Supply Chain Risk Management” (网络供应链风险管理的最佳实践), *美国国家标准和技术协会*, <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>; “OCIE’s 2015 Cybersecurity Examination Initiative” (OCIE 2015 年网络安全审查倡议), *合规监督和审查部*, 2015 年 9 月 15 日, <https://www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf>
- ¹⁴ “Security Breach Notification Laws” (安全问题通知法律), *国家各州立法联合会*, 2018 年 9 月 29 日, <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>
- ¹⁵ “2018 reform of EU data protection rules” (2018 年欧盟数据保护规则改革), *欧盟委员会*, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- ¹⁶ “The 28 member countries of the EU” (欧盟 28 个成员国), *欧盟*, https://europa.eu/european-union/about-eu/countries_en
- ¹⁷ “The GDPR: new opportunities, new obligations” (GDPR: 新机遇, 新义务), *欧盟委员会*, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf
- ¹⁸ “Art. 4 GDPR Definitions” (GDPR 第 4 条定义), *intersoft consulting*, <https://gdpr-info.eu/art-4-gdpr/>
- ¹⁹ “Art. 33 GDPR Notification of a personal data breach to the supervisory authority” (GDPR 第 33 条向监管当局通知个人信息泄露事件), *Intersoft consulting*, <https://gdpr-info.eu/art-33-gdpr/>
- ²⁰ “Art. 85 GDPR Processing and freedom of expression and information” (GDPR 第 85 条处理和表达与信息自由), *intersoft consulting*, <https://gdpr-info.eu/art-85-gdpr/>
- ²¹ “SB 318”, 2018 年, <http://arc-sos.state.al.us/PAC/SOSACPDF.001/A0012674.PDF>
- ²² “SB 62”, *南达科他州法规*, 2018 年, <http://sdlegislature.gov/docs/legsession/2018/Bills/SB62ENR.pdf>
- ²³ “Breach Notification Rule” (泄露通知法规), *美国卫生和公共服务部*, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>
- ²⁴ Gina Stevens, “Federal Information Security and Data Breach Notification Laws” (联邦信息安全与数据泄露通知法), *美国国会研究服务局*, <https://fas.org/sgp/crs/secrecy/RL34120.pdf>
- ²⁵ “Breach Notification Rule” (泄露通知法规), *美国卫生和公共服务部*, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>
- ²⁶ “State Data Breach Notification Laws” (国家数据泄露通知法律), *Foley & Lardner LLP*, 2019 年 1 月 28 日, <https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws>; 包括阿拉巴马、阿拉斯加、阿肯色、加利福尼亚、康涅狄格、华盛顿特区在内, 超过半数的州要求在发现后立即通知个人和监管机构, “不得以不合理的理由延期”。
- ²⁷ Victorianne Musonza, “Changes on the horizon for North Carolina’s data breach notification law” (北卡罗来纳州的数据泄露通知法即将发生变化), *国际隐私专家协会*, 2017 年 1 月 24 日, <https://iapp.org/news/a/changes-on-the-horizon-for-north-carolinas-data-breach-notification-law/>
- ²⁸ “Cybersecurity Requirements for Financial Services Companies” (金融服务公司的网络安全要求), *纽约州金融服务局*, <https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dsfrf500txt.pdf>
- ²⁹ 同上。第 50017 条
- ³⁰ “Certification of Enrollment Substitute House Bill 1071”, 2019 年, <http://lawfilesexet.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Passed%20Legislature/1071-S.PL.pdf>
- ³¹ “Art. 28, Processor” (第 28 条处理方), *intersoft consulting*, <https://gdpr-info.eu/art-28-gdpr/>; “Art. 32 Security of processing” (第 32 条处理安全), *intersoft consulting*, <https://gdpr-info.eu/art-32-gdpr/>
- ³² “Business Associates” (商业伙伴), *美国卫生和公共服务部*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>
- ³³ “Public Law 107-204” (美国公法 107-204), *国会图书馆*, 2002 年 7 月 30 日, <https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf>
- ³⁴ “BSA/AML Risk Assessment—Overview” (银行保密法 / 反洗钱风险评估——概述), *联邦金融机构审查委员会*, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm
- ³⁵ Agostino Carrideo, *Vendor Management: An insider’s strategies to win and create long lasting change (供应商管理: 内部人士的策略, 以赢得和创造持久的变化)*, 2015 年, 第 81 页。
- ³⁶ “Information Security Standards and Practices Guide” (信息安全标准及实践指南), *UNT System*, <https://its.untsystem.edu/sites/default/files/Information%20Security%20Standards%20and%20Practices.pdf>
- ³⁷ 同上。
- ³⁸ “Grand Theft Data” (大盗窃数据), *McAfee*, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf>
- ³⁹ “Student Privacy 101” (学生隐私 101 条), *美国教育部*, <https://nces.ed.gov/programs/ptac/pdf/issue-brief-security-training.pdf>
- ⁴⁰ “Phishing” (网络钓鱼), *联邦贸易委员会*, <https://www.consumer.ftc.gov/articles/0003-phishing>
- ⁴¹ “国家数据泄露通知法律” (State Data Breach Notification Laws), *Foley & Lardner LLP*, 2019 年 1 月 28 日, <https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws>; “Art. 5 GDPR Principles relating to processing of personal data” (第 5 条有关处理个人数据的 GDPR 原则), *intersoft consulting*, <https://gdpr-info.eu/art-5-gdpr/>; “Recital 83 Security of processing” (第 83 条规定处理安全), *Intersoft consulting*, <https://gdpr-info.eu/recitals/no-83/>

- ⁴² “HEALTH AND SAFETY CODE § 1280.15. Unlawful or unauthorized access and use or disclosure of patients’ medical information ; 调查; Report, Cal Health & Saf Code § 1280.15” (健康与安全守则 §1280.15. 非法或未经授权查阅和使用或披露患者的医疗信息; 报告, 健康与安全守则 §1280.15), *Lexis Advance*, <https://advance.lexis.com/open/document/lpadocument?pdmfid=1000522&crd=dXJuOmNvbRlbnRjZGVtOjVKNiltR1JLMS02Nk15LTgwQzgtMDAwMDAtMDA&pdofullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5J6R-GRK1-66B9-80C8-0000-00&pdcomponentid=4867>
- ⁴³ “Definition: Encryption” (定义: 加密), *ISACA*, <https://www.isaca.org/Pages/Glossary.aspx?tid=1376&char=E>
- ⁴⁴ Kevin Stine 和 Quynh Dang, “Encryption Basics” (加密基础知识), *Journal of American Health Information Management Association*, 2016 年, https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=908084
- ⁴⁵ Robert Lyon, Nick Schonning 和 Wesley David, “What is role-based access control (RBAC) for Azure resources?” (Azure 资源的基于角色的访问控制措施 (RBAC) 是什么?) *Microsoft Azure*, 2019 年 1 月 13 日, <https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>
- ⁴⁶ “Identity Authentication Best Practices” (身份验证最佳实践), *Privacy Technical Assistance Center*, 2012 年 7 月, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Identity_Authentication_Best_Practices_0.pdf
- ⁴⁷ “Intrusion Detection and Prevention Systems” (入侵侦查和防范系统), *美国国家标准和技术协会*, https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901146
- ⁴⁸ “Firewalls, intrusion prevention and VPN” (防火墙、入侵防御和 VPN), *休斯顿大学清湖分校*, <https://www.uhcl.edu/computing/information-security/tips-best-practices/firewalls>
- ⁴⁹ “Cybersecurity for Small Business” (小型企业网络安全), *美国联邦通信委员会*, <https://www.fcc.gov/general/cybersecurity-small-business>
- ⁵⁰ “Definition of: end-to-end encryption” (定义: 端到端加密), *PC Magazine*, <https://www.pcmag.com/encyclopedia/term/42602/end-to-end-encryption>
- ⁵¹ “Definition: Virtual private network (VPN)” (定义: 虚拟专用网 (VPN)), *ISACA*, <https://www.isaca.org/Pages/Glossary.aspx?tid=1969&char=V>
- ⁵² Kurtis Holland, “Incident Handling Annual Testing and Training” (事件处理年度测试和培训), *SANS Institute*, 2014 年 4 月 7 日, <https://www.sans.org/reading-room/whitepapers/incident/incident-handling-annual-testing-training-34565>
- ⁵³ “Data Breach Response: A Guide for Business” (数据泄露响应: 企业指南), *联邦贸易委员会*, <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business>
- ⁵⁴ 参见引用 NIST 和 SANS 的脚注。
- ⁵⁵ Brad Edwards, “Fired CPS Employee Steals Personal Data Of 70, 000 People, Charged With Multiple Felonies” (被解雇的 CPS 员工窃取 70,000 人的个人数据, 面临多项重罪指控), *CBS Chicago*, 2018 年 11 月 1 日, <https://chicago.cbslocal.com/2018/11/01/cps-employee-data-theft/>
- ⁵⁶ Ron Word, “2.3 million consumer financial records stolen” (230 万消费者财务记录被盗), *NBCNews.com*, 2007 年 7 月 3 日, <http://www.nbcnews.com/id/19582088/ns/>
- [technology_and_science-security/t/million-consumer-financial-records-stolen/#.XEUJgvx7nUo](https://www.nbcnews.com/id/19582088/ns/technology_and_science-security/t/million-consumer-financial-records-stolen/#.XEUJgvx7nUo)
- ⁵⁷ Andrea Peterson, “The human problem at the heart of Snapchat’s employee data breach” (Snapchat 员工数据泄露源于人为因素), *《华盛顿邮报》*, 2016 年 3 月 1 日, https://www.washingtonpost.com/news/the-switch/wp/2016/03/01/the-human-problem-at-the-heart-of-snapchats-employee-data-breach/?noredirect=on&utm_term=.27f325c145f1
- ⁵⁸ Taylor Armerding, “The 18 biggest data breaches of the 21st century” (21 世纪 18 起最大的数据泄露事件), *CSO*, 2018 年 12 月 20 日, <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>
- ⁵⁹ “Following Massive Equifax Data Breach, Gillibrand Calls On Federal Trade Commission To Conduct Immediate Review Of Consumer Data Protection At Top Consumer Reporting Agencies”, (大规模 Equifax 数据泄露后, Gillibrand 呼吁联邦贸易委员会对大型消费者报告机构的消费者数据保护机制进行直接审查), *Kirsten Gillibrand*, 2017 年 9 月 19 日, <https://www.gillibrand.senate.gov/news/press/release/following-massive-equifax-data-breach-gillibrand-calls-on-federal-trade-commission-to-conduct-immediate-review-of-consumer-data-protection-at-top-consumer-reporting-agencies>
- ⁶⁰ Pierre Thomas, “Equifax Confirms Hackers Stole Financial Data, Launches Investigation” (Equifax 确认黑客窃取财务数据并启动调查), *ABC News*, 2013 年 3 月 13 日, <https://abcnews.go.com/Politics/equifax-confirms-hackers-stole-financial-data-launches-investigation/story?id=18715884>
- ⁶¹ Kate Fazzini, “The Marriott hack that stole data from 500 million people started four years ago – investors should ask how the company missed it” (黑客从四年前开始攻击万豪酒店并窃取 5 亿人的数据——投资者应质疑万豪为何从未发现), *CNBC*, 2018 年 11 月 30 日, <https://www.cnbc.com/2018/11/30/marriott-hack-raises-questions-about-merger-diligence-tools-in-use.html>
- ⁶² Mark Hosenball, “Target vendor says hackers breached data link used for billing” (Target 公司供应商称黑客入侵了用于计费的数据链), *路透社*, 2014 年 2 月 6 日, <https://www.reuters.com/article/us-target-breach-vendor/target-vendor-says-hackers-breached-data-link-used-for-billing-idUSBREA1523E20140206>
- ⁶³ Maggie McGrath, “Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming” (因信用卡信息泄露 Target 公司利润下跌 46% 且影响仍可能扩大), *福布斯*, 2014 年 2 月 26 日, <https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#34b1d1187326>
- ⁶⁴ “AG Stein Joins 46 States and DC in \$18.5m settlement with Target Corporation” (AG Stein 与其他 46 个州和华盛顿一道与 Target 公司达成 1,850 万美元和解), *美国总检察长 Josh Stein*, 2017 年 5 月 23 日, [https://www.ncdoj.gov/News-and-Alerts/News-Releases-and-Advisories/AG-Stein-Joins-46-States-and-DC-in-\\$18-5M-Settleme.aspx](https://www.ncdoj.gov/News-and-Alerts/News-Releases-and-Advisories/AG-Stein-Joins-46-States-and-DC-in-$18-5M-Settleme.aspx)
- ⁶⁵ “2018 Cost of a Data Breach Study: Global Overview” (2018 年数据泄露成本研究: 全球概览), *Ponemon Institute*, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf