IMMC 2020 Greater China Problem D (Winter) （English 简体 繁体）

Incentive Strategy of Cyber Insurance

Cyberattack is now one of the most significant emerging risks that all organizations ranging from governmental entities to private companies around the world have to deal with seriously[1]. The chance of being attacked and the strength of defending against an attack vary significantly across them. A succeeded attack can cause substantial damages to the victim, such as loss of valuable data, repair and replacement of equipment, regulatory fines and penalties, litigation costs, damaged brand and reputation, production disruption, loss of customers, and so on.[2] According to one report by IBM, the global average cost of a data breach in 2018 increased by 6.4% over the previous year to US$3,860,000, and the average cost for each lost or stolen record containing sensitive and confidential information increased by 4.8% to US$148.[3]

In 2013, Target, a US retailer, was the victim of one of the largest data breaches in the history of the retail industry. According to the company's report, the POS system in over 1,800 stores was infiltrated by malware and around 40 million customers' credit and debit cards became susceptible to fraud. Investigation officials suspected that the hackers broke into Target's network using passcode credentials stolen from Fazio Mechanical Services, a Pennsylvania-based third party supplier of Target's computer systems. Target spent around US$61 million responding to the breach according to its fourth-quarter 2013 financial statement.[4]

In 2017, Mondelez International, a global snack-food manufacturer and one of the 100 largest U.S. companies by market capitalization, was a victim of the NotPetya malware attacks. The

[1] https://www.ogcio.gov.hk/en/news/legco_papers/2019/02/doc/lb_20190218.pdf
[2] https://doi.org/10.1787/9789264282148-en
[3] https://www.ibm.com/security/data-breach
[4] https://en.wikipedia.org/wiki/Supply_chain_attack

company reported that 1,700 computer servers and 24,000 laptops were permanently disabled by the virus and estimated the total costs US$100 million.[5]

As a concequence of rampant attacks from cyber space, the demand for cyber insurance is increasing. It is estimated that the total revenue of the global cyber insurance market will experience 33.8 percent compound annual growth, increasing from US$2.92 billion in 2019 to US$16.7 billion by 2024.[6] The insured expect to receive some monetary reimbursement for the damages after being attacked. In addition, the insured have access to expert advice offered by the insurance company that helps strengthen their defense against cyberattacks.

However, small and medium-size enterprises are vulnerable to cyberattacks and less than 5% of them have cyber insurance.[7] As in the case of Target, the break-in in a small company caused severe damages to partners in the supply network. Supply chain attacks are in fact a commonly deployed cyberattack tactic and increased by 79 percent in 2018.[8]

Consider one giant company with many small and medium-size suppliers. To protect itself against supply chain attacks, the giant company plans to purchase only from the suppliers who have adequate cyber insurance coverage. To provide incentives to suppliers, the giant company is willing to pay part of the cyber insurance premium for each supplier. How do you determine the premium that the giant company should pay for each supplier? Please provide your mathematical modeling solution and suggest the incentive strategy of cyber insurance for the giant company.

Submission

Your solution paper should include a 1-page Summary Sheet. The body cannot exceed 20 pages for a maximum of 21 pages with the Summary Sheet inclusive. The appendices and references should appear at the end of the paper and do not count towards the 21 pages limit.

---

[5] https://en.wikipedia.org/wiki/Petya_(malware)
[6] https://www.marketwatch.com/press-release/338-growth-for-cyber-insurance-market-size-to-2024-2019-02-08
[7] https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[8] https://en.wikipedia.org/wiki/Supply_chain_attack

IMMC 2020 中华赛 D 题（冬季赛） （English 简体 繁体）

网络保险激励策略

网络风险现在是从政府实体到私人公司的所有组织所必须认真应对的最重要的新兴风险之一[1]。被攻击的机会和防御的实力在组织间会有很大差别。一次成功的攻击可能会给受害者造成重大损伤，例如珍贵数据的丢失，设备的维修和更换，合规罚款和罚金，诉讼费用，品牌和声誉受损，生产中断，客户流失，等等[2]。根据 IBM 的一份报告，2018 年全球数据泄露的平均成本比上一年增长 6.4%，达到 386 万美元，每条包含敏感和机密信息的丢失或被盗记录的平均成本增长了 4.8%，至 148 美元[3]。

2013 年，美国零售商塔吉特（Target）成为其中一宗零售业历史上最大的数据泄露事件的受害者。据公司报告，超过 1800 家商店的 POS 系统被恶意软件渗透，大约 4000 万客户的信用卡和借记卡可能遭受欺诈。调查官怀疑，黑客利用从宾夕法尼亚州塔吉特计算机系统的第三方供应商法齐奥（Fazio）机械服务公司窃取的密码凭证闯入塔吉特网络。根据其 2013 年第四季度财务报表，塔吉特公司花费了约 6,100 万美元来应对这次数据泄露事件[4]。

2017 年，全球休闲食品制造商和美国市值最大的 100 家公司之一的亿滋国际（Mondelez International）成为 NotPetya 勒索软件攻击的受害者。该公司报告称，攻击病毒永久禁用了 1,700 台计算机服务器和 24,000 台笔记本电脑，估计总成本为 1 亿美元[5]。

网络攻击的肆虐，造成对网络保险的需求不断增长。据估计，全球网络保险市场的总收入复合年增长率将是 33.8%，从 2019 年的 29.2 亿美元增长到 2024 年的 167 亿美元[6]。受保险人预期

[1] https://www.ogcio.gov.hk/sc/news/legco_papers/2019/02/doc/lb_20190218.pdf
[2] https://doi.org/10.1787/9789264282148-en
[3] https://www.ibm.com/security/data-breach
[4] https://en.wikipedia.org/wiki/Supply_chain_attack
[5] https://en.wikipedia.org/wiki/Petya_(malware)

将在遭受攻击后获得部分赔偿。此外，受保险人可以获取保险公司提供的专家建议，以帮助他们加强防御网络攻击的能力。

然而，中小企业在网络攻击面前却是脆弱的，只有不到 5%的中小企业拥有网络保险[7]。例如在 Target 网络攻击事件中，正是一家小公司的遭受入侵，对整个供应链网络中的众合作伙伴造成了严重损害。实际上，供应链攻击是网络攻击中被普遍采用的策略，在 2018 年增长了 79%[8]。

考虑一家拥有许多中小型供应商的巨型公司。为了保护自己免受供应链攻击，这家巨型公司计划只从已拥有足够网络保险的供应商那里进行采购。为了激励供应商，这家巨型公司愿意为每一家供应商支付部分网络保险费。您如何确定这家巨型公司应为每家供应商支付的保费？请建立您的数学建模解决方案，并为这家巨型公司提供网络保险激励策略。

提交

您的解决方案论文应包括 1 页的摘要，正文不能超过 20 页，含摘要最多 21 页。 附录和参考资料应出现在正文之后，不算在 21 页的限制之内。

[6] https://www.marketwatch.com/press-release/338-growth-for-cyber-insurance-market-size-to-2024-2019-02-08
[7] https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[8] https://en.wikipedia.org/wiki/Supply_chain_attack

IMMC 2020 中華賽 D 題（冬季賽） （English 简体 繁體）

網絡保險激勵策略

網絡風險現在是從政府實體到私人公司的所有組織所必須認真應對的最重要的新興風險之一[1]。被攻擊的機會和防禦的實力在組織間會有很大差別。一次成功的攻擊可能會給受害者造成重大損傷，例如珍貴數據的丟失，設備的維修和更換，合規罰款和罰金，訴訟費用，品牌和聲譽受損，生產中斷，客戶流失，等等[2]。根據 IBM 的一份報告，2018 年全球數據外洩的平均成本比上一年增長 6.4%，達到 386 萬美元，每條包含敏感和機密信息的丟失或被盜記錄的平均成本增長了 4.8%，至 148 美元[3]。

2013 年，美國零售商塔吉特（Target）成為其中一宗零售業歷史上最大的數據外洩事件的受害者。據公司報告，超過 1800 家商店的 POS 系統被惡意軟件滲透，大約 4000 萬客戶的信用卡和借記卡可能遭受欺詐。調查官懷疑，黑客利用從賓夕法尼亞州塔吉特計算機系統的第三方供應商法齊奧（Fazio）機械服務公司竊取的密碼憑證闖入塔吉特網絡。根據其 2013 年第四季度財務報表，塔吉特公司花費了約 6,100 萬美元來應對這次數據外洩事件[4]。

2017 年，全球休閒食品製造商和美國市值最大的 100 家公司之一的億滋國際（Mondelez International）成為 NotPetya 勒索軟件攻擊的受害者。該公司報告稱，攻擊病毒永久禁用了 1,700 台計算機服務器和 24,000 台筆記本電腦，估計總成本為 1 億美元[5]。

網絡攻擊的肆虐，造成對網絡保險的需求不斷增長。據估計，全球網絡保險市場的總收入複合年增長率將是 33.8%，從 2019 年的 29.2 億美元增長到 2024 年的 167 億美元[6]。受保險人預期將在遭受攻擊後獲得部分賠償。此外，受保險人可以獲取保險公司提供的專家建議，以幫助他們加強防禦網絡攻擊的能力。

---

[1] https://www.ogcio.gov.hk/tc/news/legco_papers/2019/02/doc/lb_20190218.pdf
[2] https://doi.org/10.1787/9789264282148-en
[3] https://www.ibm.com/security/data-breach
[4] https://en.wikipedia.org/wiki/Supply_chain_attack
[5] https://en.wikipedia.org/wiki/Petya_(malware)
[6] https://www.marketwatch.com/press-release/338-growth-for-cyber-insurance-market-size-to-2024-2019-02-08

然而，中小企業在網絡攻擊面前卻是脆弱的，只有不到 5％的中小企業擁有網絡保險[7]。例如在 Target 網絡攻擊事件中，正是一家小公司的遭受入侵，對整個供應鏈網絡中的眾合作夥伴造成了嚴重損害。實際上，供應鏈攻擊是網絡攻擊中被普遍採用的策略，在 2018 年增長了 79％[8]。

考慮一家擁有許多中小型供應商的巨型公司。為了保護自己免受供應鏈攻擊，這家巨型公司計劃只從已擁有足夠網絡保險的供應商那裡進行採購。為了激勵供應商，這家巨型公司願意為每一家供應商支付部分網絡保險費。您如何確定這家巨型公司應為每家供應商支付的保費？請建立您的數學建模解決方案，並為這家巨型公司提供網絡保險激勵策略。

提交

您的解決方案論文應包括 1 頁的摘要，正文不能超過 20 頁，含摘要最多 21 頁。 附錄和參考資料應出現在正文之後，不算在 21 頁的限制之內。

[7] https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[8] https://en.wikipedia.org/wiki/Supply_chain_attack