



Immaturity & Moral Hazard in the Cyber Insurance Market

By **Kevin A. Sesock** – ISSA member, Oklahoma City Chapter



Cyber insurance is an insurance market growing in size, complexity, and price at a time when cyber threats cause fear, uncertainty, and doubt throughout the market and among legislators, cybersecurity advocates, and the news media. The author argues that despite the perceived usefulness of such a policy type, cyber insurance policies remain an unsound investment for most organizations in most markets.

Abstract

Cyber insurance is an insurance market growing in size, complexity, and price at a time when cyber threats cause fear, uncertainty, and doubt throughout the market and among legislators, cybersecurity advocates, and the news media. It is only recently that high-profile breach claims such as Target, 21st Century Oncology, and others have completely developed, and an understanding of the cost and benefits of cyber insurance begin to come into focus, including reputational damage, the risk of bankruptcy, loss in business and customer loyalty, and others.

Reputational damage, loss of customer loyalty, and dips in sales are often overhyped, while claim recoveries are small compared with the cost of premiums. At this time, these factors contribute to an overall lack of maturity in the market, while the overall cost benefit of cyber insurance and the presence of moral hazard indicate that most organizations, especially small and medium businesses that lack any kind of cybersecurity maturity, should not invest in cyber liability or

cyber insurance; instead, utilize those resources for the benefit of improving their cyber risk-management mitigation and avoidance techniques.

Relatively new to the world of insurance is cyber insurance, sometimes called cyber liability insurance. These policies are designed to transfer risk from the insured to the insurance company in the form of monetary compensation for the company and its customers in the event of various forms of data breach. Despite the perceived usefulness of such a policy type, and primarily due to lack of maturity in the cyber insurance market, but also due to the interconnectedness of all insureds, cyber liability insurance policies remain an unsound investment for most organizations in most markets.

Current events

Recently, noted security researcher Brian Krebs reported on The National Bank of Blacksburg's breach that started in May 2016, most likely by Russian hackers intent on siphoning money out of the bank by socially engineering employees

and gaining access to bank patrons' account details. After the breach, the bank's insurer, Everest National Insurance Company, denied the claim and the bank subsequently filed suit against Everest. The root cause of the disagreement now working its way through the court system is based on the insurer disagreeing on root versus proximate cause. Krebs castigates the insurance company's lack of standardization in policies that makes the job of purchasing policies extremely complex for most businesses [8].

Similarly, while the Target Corporation data breach of 2013 is by now old news, it has taken many years for the costs borne by Target, as well as Target's cyber insurers, to be fully realized and the final price tag to be tallied. The current newsworthiness of this hack more stems from the final price tag and not from any technical details regarding the attack itself, as the technical details are well-known and by 2019 have been discussed at length. As late as mid-2017, the final settlements were entering the news and as of 2018, Target has all but ceased even utilizing the word "breach" in its annual financial statements. Ultimately, Target Corporation's direct costs reached approximately \$200M, with an additional \$92M in costs that were borne by Target's various cyber insurers.

These examples, especially Target, continue to be used as motivators by agents and corporations for ongoing investment in cyber insurance for organizations of all sizes.

Market status

Cyber insurance policy sales are one of the smaller sectors of the insurance market, yet the most rapidly growing [9]. Customers, primarily in the US, are taking up cyber insurance policies at an accelerating rate, primarily driven by state-level breach notification laws, with EMEA countries also experiencing growth, albeit at a slower pace than US-based insureds [7]. On the supply side, carriers are offering products with

expanding coverage sublimit categories, while pricing, availability, and market differentiation vary wildly across markets, customers, and firm sizes [13].

Cyber risk management and risk transfer

The cyber insurance market forms a small but growing niche for insurers and a seemingly important protection mechanism for customers. In an idealized model, customers would practice diligent risk management practices with deliberate decision making regarding their cyber-security posture. Utilizing ISO 31000 terminology, and in the parlance of enterprise risk managers, these customers would purchase cyber insurance to transfer residual risk, as a last step before risk acceptance. This allows the insured to focus on directly manageable risk and represents a maturing risk management culture in an organization with more than adequate cybersecurity funding, governing board-level insight into cyber risk, and strategic-minded staff.

However, cyber insurance is not a panacea and the real world is rarely so optimal. With cyber being a new insurance market, it has rapidly morphed and shows every indication of continuing to evolve more rapidly than consumers are prepared for, but not nearly as quickly as the threat landscape does. As new threats emerge, insurers scramble to address these new threats and remain competitive in an extremely dynamic market by offering new products, sublimits, and more value-added solutions (such as risk prevention tools, training, and support) in a lag behind the emerging threats.

Analysis

One of the primary issues to contemplate within not just cyber insurance but in all insurance is the concern known as *moral hazard*. Moral hazard is a form of over-correction by insureds (i.e., the tendency for one to relax one's own risk



Join Today: www.issa.org/join

Regular Membership \$95*
(+ Chapter Dues: \$0-\$35*)

Members Join ISSA to:

- Earn CPEs through Conferences and Education
- Network with Industry Leaders
- Advance their Careers
- Attend Chapter Events to Meet Local Colleagues
- Become part of Special Interest Groups (SIGs) that focus on particular topics

CISO Executive Membership \$995
(Includes Quarterly Forums)

*US Dollars/Year

management posture and become complacent regarding one's own risk, even consciously due to the fact that one no longer has to face the consequences of one's actions). A more traditional insurance example might be if one has comprehensive coverage on her vehicle, she may be more willing to park it outside during a hail storm or neglect to lock the doors in a high-crime neighborhood. Moral hazard stems from information asymmetry: the insurer believes you are going to take the necessary steps to protect your investment, whereas you have less incentive to do so since you have been separated from the consequences of your actions.

Cyber insurance moral hazard

Cyber insurance is not immune from the threat of moral hazard. According to Schwartz and Sastry, the very act of purchasing cyber insurance decreases the overall cybersecurity of not just the insureds purchasing the insurance, but all nodes on the network as a whole. This is due to the interdependent nature of the Internet, as those with insurance and low security will decrease security for their neighbors and partners that are properly protected [17]. In their

models they utilized virus and malware infections, and the decrease in overall cybersecurity for the Internet as a whole is indeed similar to a loss of herd immunity in populations with sufficient individuals that eschew vaccinations for moral or religious reasons.

Similarly, Lang and Lui utilized game theory modeling to analyze security investment amongst disparate insureds of varying sizes, and demonstrate that while a competitive market can potentially encourage better network security amongst individual insureds, this is only without the presence of moral hazard. This mathematically implicates that the source of this degradation in overall security for all members of a network stems ultimately from moral hazard [23] and not from other network or policy effects. This means that to protect everyone on the Internet, insurers must work to eliminate moral hazard by improving rating, loss control, and being prepared to deny coverage to customers that fail to properly protect themselves.

The case for small and medium business cyber insurance

Proponents of cyber insurance continue to encourage organizations to jump on the cyber insurance bandwagon, and there has been renewed focus on the impacts of unprotected systems and lack of proper cyber insurance on small and medium businesses. Zaleski highlights particularly concerning statistics about the impacts of cybersecurity breaches on small businesses, with particular respect to showcasing the benefits from Senate Bill 770 from the 115th Congress, the NIST Small Business Cybersecurity Act (alternatively titled the Mainstreet Cybersecurity Act). Zaleski repeats a claim that the National Cyber Security Alliance (NCSA) found that 60 percent of small firms go out of business six months after a breach [24].

The Better Business Bureau found through self-reported surveys that 37 percent of all hacked small businesses lost money, with an average of respondents reporting losses of over \$79,000, and median of reported losses of \$2,000 [6]. Interestingly, the disparity between the average and median indicates large outliers in this report's data, and indeed, as this is self-reported survey data, the losses may be misleading towards the high end. The report indicates a large breach of nearly \$1M may have skewed the data. Median reported losses in the \$2,000 range is consistent with payouts for the most common type of non- or semi-targeted attacks usually associated with broad campaigns of phishing (and lower-level spearphishing), ransomware infections, and other less sophisticated threats.

Cost benefit of cyber insurance

No discussion of cyber insurance is complete without understanding the premium cost to the insured versus the coverage. The costs associated with cyber insurance premiums are dependent on the coverage selected for the insured, which essentially is defined by the amount of data the insured has, and ultimately the size of the insured itself. Typically, an insurer will rate the risk for an insured based on two primary factors.



ISSA Thought Leadership Series

The 7 Deadly Sins of Insiders: Why They Become Threats & How to Defend

60-minute Live Event: Wednesday, October 9, 2019

10 a.m. US-Pacific/1 p.m. US-Eastern/6 p.m. London

In this panel webinar, ObserveIT's head of security, Chris Bush, will interview two experts on the topic of the risk from insider threats. We will illuminate the seven common motives—also known as the seven deadly sins—that influence insider threats and share best practices for defending against them. We will explore what makes insider threats so different from traditional external threats. We'll also cover:

- The seven most common motives for insider threats
- How to detect and investigate insider threats efficiently and accurately
- What to do about insider threats in your supply chain
- How to fit insider threat protection into your broader security program
- Legal and privacy concerns that often arise within insider threat programs

Generously supported by



[CLICK HERE TO REGISTER.](#)

For more information on these or other webinars:

ISSA.org => [Events](#) => [Web Conferences](#)

DON'T BE OUTPACED

A new generation of cyber-threat has emerged. Machine-speed threats can cripple systems in seconds and bring your business to a halt.

Powered by AI, Darktrace responds to attacks in seconds – allowing you to regain the advantage.

Learn more at darktrace.com



DARKTRACE
World-Leading Cyber AI

TIME	AMOUNT	DESCRIPTION	SOURCE
2013	\$17M	Recovery and business costs	[20]
2014	\$145M	Recovery and business costs	[20]
April 2015	\$10M	Customer class action lawsuit settlement	[19]
August 2015	\$67M	Fees and fines to Visa	[10]
December 2015	\$39.4M	Bank class action lawsuit settlement	[18]
May 2017	\$18.5M	47-state settlement	[2]
Total	\$296.9M	Total cost pre-insurance	

Table 1: Target breach costs over time with insurance recoveries

First, the impact of a loss, such as the number of PII records the insured retains multiplied by the average cost of each record, usually estimated by data type (health-, financial-, and credit-related data being higher value than basic contact information). Secondly, the likelihood of a loss, usually determined by a light cybersecurity review typically collected via a high-level underwriting questionnaire.

According to The Organisation for Economic Co-operation and Development (OECD), prices vary wildly and are climbing. High-risk markets such as health care are seeing premiums increase due to customers needing to increase coverage, and also decreasing competition and insurers exiting cyber insurance due to high-profile breaches [13]. Several reports indicate that \$1M in coverage can vary between \$5K-50K per year, depending on the size of the customer. These premiums "... for the same amount of coverage [are] three times more expensive than general liability coverage and six times more

expensive than property coverage" [13]. In addition, the OECD concludes that "... the cost per million of cyber liability insurance has increased by over 200 percent since Q1 2012, relative to a 17 percent decline in US commercial property and casualty pricing" [13].


Large market cap corporate breaches and historical precedent for cyber insurance

Target’s 2012 breach provides a fully developed example of claims development and as the largest corporate entity to

date to suffer from such an attack, provides a good example of large-cap cyber claims. As per table 1, Target’s direct costs for the breach have reached a total of approximately \$296.9M. Target had a total of \$100M in cyber insurance (with a \$10M self-insured retention) spread out over multiple insurers, and \$65M in directors and officers insurance coverage, allowing Target to recover \$92M in their breach costs according to their own SEC filings. This brings the net total to Target’s bottom line, and ultimately their shareholders, to just over \$200M. What is not clear from these numbers are the calculations Target’s staff conducted to plan for risk transfer and analyze the cost versus benefit of the annual cyber insurance premiums versus the coverage limits that could have reduced Target’s own costs. These calculations coupled with the other controls that would have mitigated, avoided, and reduced their risks could have painted a much different financial picture for Target if plans were properly implemented ahead of time. Therefore, the ultimate lesson after five years from the Target breach is the disparity between the following cost estimates: (1) the initial rhetorical cost estimate portrayed in the new media, (2) the ultimate cost of the breach itself before insurance recoveries, and (3) the disparity between the cost of the breach and the limits of coverage the insured had paid for.

Ultimately, in the largest, most complex events for the larger insureds, it will take several years for this complete picture to form. For small and medium businesses, breach response and recovery, notification, and finally claims development may be complete and put to rest in mere weeks. With the frequency of breach notifications going to customers reaching a deafening crescendo, customers may overall be ignoring or tuning out all but the largest, highest-profile breaches, and small business insureds likely only need concern themselves with the most basic of recovery activities such as notification and credit monitoring.

In summary, reputational damage, including lost sales that are not the direct result of business interruption or inability to conduct business may simply not be as major of a threat as described in the rhetoric. While consumer complacency about cyber threats is worrisome, this also illustrates a feedback loop within moral hazard itself: human nature will continue to reward cyber risk transfer in lieu of cyber risk mitigation without the presence of incentives or deterrents.




Infosec Book Reviews

Have you read an excellent information security book of value to ISSA members? You are invited to share your thoughts in the ISSA Journal.

- Summarize contents
- Evaluate interesting or useful information
- Describe the value to information security professionals
- Address any criticisms, omissions, or areas that need further development

Review should be 500-800 words, including short bio, photo, and contact email. Submit your review to editor@issa.org.



DEVELOPING AND CONNECTING
CYBERSECURITY LEADERS GLOBALLY

	IMMATURE/INSECURE	MATURING/SECURING	MATURE
Does Not Purchase	Uninformed and Unable/Unwilling¹ Potential cyber insurance customers had “insufficient knowledge” of their own risks to buy insurance or were deemed unacceptable risks by insurers.	Security Investors² Would rather invest as much of limited resources into security improvements, mitigation, and avoidance efforts as opposed to transference.	Risk Accepters All risk is mitigated, avoided, and finally accepted. Risk transfer is used temporarily or not at all and only with positive cost-benefit analysis.
Purchases	Fearfully Unaware Supposition that this group purchases out of fear of cyber risk and not as a legitimate risk management effort.	Stop Gappers Organizations in this category may be on the path of addressing outstanding cyber risk but may only be executing beginning stages of their plan, and require cyber insurance as a temporary measure.	Risk Transferrers Whether because of a high-risk market, such as health or retail, or because of unavoidable, unmitigable risks, these organizations make the deliberate choice to transfer an appropriate amount of risk after analyzing the costs.

1 Kshteri reports on a survey conducted by Marsh, where 49 percent of respondents were unable to determine what cyber insurance they need [9].
 2 Ponemon reports that from those that will not purchase cyber insurance, too high of a price and too many restrictions are principal reasons potential insurers decline policies [14].

Table 2 – Classifications of cyber insurance customers vs. risk management maturity

Erosion of business value and failure in the aftermath of a breach

To further unpack the rhetoric over reputational damage or lost sales, these coverages extend beyond business interruption and are intended to fill in the gap while a business works to repair its corporate image and address the loss of customers[16]. Some policies even provide public relations services as part of breach response, often tied in with corporate communication, call center, and notification services [16]. According to ranking member Nydia Velazquez (D – N.Y.) of the US House of Representatives Committee on Small Business in a July 26, 2017, hearing, “Small businesses that lose customer information when their security is breached suffer significant costs financially and the loss of customer trust” [21].

To return to the Target example for a moment, and other than direct costs, then what of Target’s reputational damage, resulting in lost sales, opportunity costs, and lowered share price? Target did post a 46 percent decline in sales for the same quarter one year after their breach, and a 10 percent drop in its share price, but their share price rebounded in February and by 2018 their fourth-quarter revenue had risen above pre-breach levels.

Clearly, Target’s share price, lost business, and reputational losses and those of a small business are not comparing apples to apples. However, Drinkwater questions the threat of reputational cost and loss of sales and believes the threats to be hype [5]. Likewise, Mason demonstrates through analysis of publicly available stock prices that for large-cap enterprises involved in high-profile breaches (Target, Home Depot, and Sony, to name a few), the stock price drop due to the breach is negligible and recovers quickly [11].

Resolution

Through this analysis it has become clear that cyber insurance has its place for certain organizations that practice diligent risk management practices. However, the vast majority

of organizations, and especially small and medium businesses with more limited resources, may find themselves at a crossroads on whether to invest in cybersecurity improvements or to pay a cyber insurance premium. In these cases purchasing cyber insurance does little to improve an individual organization’s cybersecurity posture, and even more harm to society writ large.

Benefits even without risk transfer

An organization that carefully and continuously considers and plans for its own risk is by definition engaging in enterprise risk management. Meland, et al actually drew the conclusion that “... even for organizations that did not end up buying insurance, there were still positive effects from the consideration process, since it brought attention and awareness of cybersecurity to the management level and across the organization” [12]. This presents an interesting quandary with respect to organizations that are not mature enough to go through the consideration process: insurance customers that do not understand cyber risk well will fall under one of two camps: those that purchase cyber insurance out of fear, and those that are blissfully unaware of cyber risk in the first place. In both cases, becoming more aware of their own organization’s risk profile will only serve to mature their risk management posture and allow the organization to better mitigate and avoid risk as opposed to transfer it, except as a stop-gap measure. Table 2 illustrates a possible categorization and descriptions of the types of customers in each camp, along a simple spectrum of risk management maturity.

Debunking small business impacts

While a smattering of business failures purporting to be either proximally or directly attributable to breaches are able to be located, the statistic of 60 percent six months after a breach is directly refuted by the National Cyber Security Alliance themselves on their own website, and a legitimate source for this claim cannot be located [3].

Continued on page 36

Immaturity and Moral Hazard in the Cyber Insurance Market

Continued from [page 19](#)

The scare tactics towards small and medium business owners and managers are especially bad amongst other players in the market with extreme profit-motive, notably cybersecurity-focused IT managed services providers, and not just insurers. Unsourced statistics citing bankruptcy and business failure rates for companies experiencing a breach are designed to lead business owners to believe that their business will almost certainly be insolvent in mere months in the event of a breach but are often completely without actual research or data. 21st Century Oncology, which suffered a data breach of 2.2M patient personal health records in 2015, and which filed for Chapter 11 bankruptcy protection in 2017, can be found cited as an example of data breaches causing business deterioration and failure [4].

One should note, however, that 21st Century Oncology, in their own Chapter 11 bankruptcy filings, states a host of other causes of their bankruptcy filing, including changing political factors, declining revenue per treatment, and changing insurance reimbursement rates. The company has experienced other legal problems unrelated to its 2015 data breach, including allegations it billed government medical programs unnecessarily, leading to a \$55M out-of-court settlement. Summarily, to conclude that 21st Century Oncology is the poster-child for data breach bankruptcy risks by those selling cybersecurity services is specious, at best.

21st Century Oncology had cyber insurance through Beazley, and as part of the bankruptcy a settlement was reached

with the breach plaintiffs, which allowed for some of the policy coverage details to be revealed. 21st Century, at the time of the settlement, had \$4.2M remaining coverage including \$2.4M for the regulatory sublimit (covering fines and settlements with regulatory compliance agencies such as HHS), all through Beazley Specialty. With \$773K of cyber-specific claims outstanding at the time of this filing, plus outstanding regulatory settlements of no more than \$2.5M, 21st Century Oncology was able to absorb their breach expenses utilizing their cyber insurance policy [1]. This puts 21st Century in the “Stop Gappers” category and demonstrates that while their cyber insurance was sufficient for their needs at the time of this specific breach, 21st Century allowed a large, critical breach to happen.

Claims adjusting and the made-whole doctrine

Even if the insurer were to pay out in the event of a breach (which is not guaranteed, as in the case of *Kreb’s* analysis), this only takes the insured back to the point where they are made whole, but does not improve their cybersecurity standing, address their vulnerabilities, or prevent future attacks. Incidentally, while the National Bank of Blacksburg believed they were purchasing insurance that would make them whole, the dispute highlights the pitfalls within cyber insurance and places Blacksburg somewhere between “Fearfully Unaware” and “Uninformed and Unable.”

Large-cap insurance bottom-line impact

To return one last time to the finalized Target data breach costs, clearly \$200M in lost direct costs, plus noticeable yet temporary drops in both sales and shareholder value, are measurable detriments to a company’s bottom line, but these impacts have not significantly weakened Target or caused massive damage to the corporation and have clearly not risen to the \$1B in costs originally predicted [22]. While it’s clear that Target’s breach was partially self-inflicted due to poor internal controls, it is also worth questioning if, in fact, these weakened postures were due to the illusion of safety because of the presence of a cyber liability insurance policy.

Moral hazard makes it clear that purchasing insurance is no replacement for proper risk management, and it is clear in hindsight that the amount of risk that was actually transferred was not the amount of residual risk Target was actually retaining. Taking all of this into account, and considering the lack of long-term damage to reputation, share price, and sales, coupled with the ultimate direct costs of the Target claim, \$200M spread out over several years for the world’s third-largest retailer with approximately \$75B in annual sales, the overall impact on a large-cap enterprise of cyber insurance in the event of a claim is relatively negligible.

NORTH TEXAS ISSA
#NTXISSA

#NTXISSA C S C 7

Cyber Security Conference
November 15th, 2019
2800 E Spring Creek Pkwy,
Plano, TX 75074

Register @ NTXISSA.org

Cost-benefit analysis

With prices of cyber insurance fluctuating wildly—exorbitant compared to other insurance products and difficult to estimate based on specific needs, customer-size, market, and cybersecurity standpoint—customers will have an increasingly simple choice about where to invest limited cybersecurity funds, especially smaller, less well-funded companies and organizations. With average breach claim payouts being lower for small and medium businesses, and the cost of mitigation and avoidance efforts already being steep, small and medium businesses especially should avoid the increasing cost of cyber insurance and instead invest in simple cybersecurity tools, such as modern firewalls, enduser training, anti-virus, and cybersecurity professional services such as audits, configuration assistance, and monitoring.

Conclusion and the future

Harold Tipton, the former executive director of the (ISC)² organization, has spoken out directly against cyber insurance and refused to procure cyber insurance for the (ISC)² during his tenure, noting in one article that “A company should not let complacency set in just because they are insured” [15]. Not only is this sentiment borne out by the lack of data supporting the purchase and implementation of cyber insurance in today’s market, but also by the risks associated with each organization’s interconnectedness.

A number of factors could change these recommendations in coming years, such as laws causing major sea changes in the market. Potential changes could include a shift to a compulsory insurance market (similar to how all drivers are required to retain auto liability insurance), cost caps or financial assistance for small and medium businesses, or more mature pricing of risk by cyber insurers themselves. Until the market adapts, however, cyber insurance is still too immature and

complex to offer protection to interconnected firms writ large. In the vast majority of cases, the costs that would normally be spent on cyber insurance should instead be invested in an organization mitigating and avoiding cyber risk, especially in the absence of a robust risk management culture. Only in the case of an organization with a mature or maturing risk management culture should risk transfer to an insurer be considered an option, and even then, be carefully considered and used almost as a last resort.

References

1. 21st Century Oncology Holdings, Inc., et al., Debtors, 2017 – https://s3.amazonaws.com/assets.fiercemarkets.net/public/004-Healthcare/external_Q42017/21CO_classaction.pdf.
2. Abrams, R. , “Target to Pay \$18.5 Million to 47 States in Security Breach Settlement,” NY Times (23 May 2017) – <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>.
3. Beffa, J., “National Cyber Security Alliance Statement Regarding Incorrect Small Business Statistic,” Stay Safe Online (May 8, 2017) – <https://staysafeonline.org/press-release/national-cyber-security-alliance-statement-regarding-incorrect-small-business-statistic/>.
4. Dobran, B., “Cyber Tragedy: 5 Stages of Business Deterioration after a Data Breach,” PhoenixNAP (October 19, 2017) – <https://phoenixnap.com/blog/business-deterioration-after-a-data-breach>.
5. Drinkwater, D., “Does a Data Breach Really Affect Your Firm’s Reputation?,” CSO Online (January 7, 2016) – <https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html>.
6. Fanelli, B. et al, “2017 State of Cybersecurity among Small Businesses in North America,” Council of Better Business Bureaus, Arlington, VA, 2017.



Write for your ISSA Journal...

Advance your career • Gain chapter, national, and global recognition
 Help others benefit from your expertise • Indexed in EBSCO database

- Legal & Public Policy
- Cloud
- Infosec Basics
- Cryptography
- Privacy
- Internet of Things
- The Toolbox
- Information Security Standards
- The Business Side of Security
- Security DevOps
- Looking Forward

- **Monthly topics**
Expanded theme descriptions [here](#).
- **Choose your own topic**
Have a different infosec topic in mind? Go ahead and submit it.
- **Mentor program**
We will pair you up with an experienced writer in [Friends of Authors](#)

If you have an infosec topic that does not align with the monthly themes, please submit. All articles will be considered.



~Thom Barrie, [Editor](#)

It's Your Journal – Contribute Your knowledge & Expertise

7. Hiscox, "The Hiscox Cyber Readiness Report 2017," Hiscox – <https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf>.
8. Krebs, B., "Hackers Breached Virginia Bank Twice in Eight Months, Stole \$2.4M," Krebs on Security (July 18, 2018) – <https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/>.
9. Kshetri, N., "The Economics of Cyber Insurance," IT Professional, vol. 20, no. 6, pp. 9-14, November 2018.
10. Malcolm, H., "Target Settles with Visa over Data Breach," USA Today (18 August 2015) – <https://www.usatoday.com/story/money/2015/08/18/target-settles-visa-over-data-breach/31911123/>.
11. Mason, S., "Impact on Stock Following a Data Breach – Dec 2016" (December 27, 2016) – <http://seanmason.com/2016/12/27/impact-on-stock-following-a-data-breach-dec-2016/>.
12. Meland, P. H. et al, "Facing Uncertainty in Cyber Insurance Policies," in STM: International Workshop on Security and Trust Management, Oslo, Norway, 2017.
13. OECD, "Enhancing the Role of Insurance in Cyber Risk Management," OECD Publishing, Paris, 2017 – <https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf>.
14. Ponemon Institute, "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," Experian (7 August 2013) – https://www.experian.com/innovation/thought-leadership/ponemon-study-managing-cyber-security-as-business-risk.jsp?ecd_dbres_cyber_insurance_study_ponemon_referral.
15. Pratt, M. K., "Cyberumbrella," Computerworld, pp. 24-25 (January 12, 2012) – <https://www.computerworld.com/article/2500188/cyberumbrella.html>.
16. Romanosky, S. et al, "Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?," RAND Corporation Justice, Infrastructure, and Environment, 2017.
17. Schwartz, G. A. and S. S. Sastry, "Cyber Insurance Framework for Large- Scale Interdependent Networks," in Proceedings of the 3rd International Conference of High Confidence Networking Systems, Berlin, 2014.
18. Stempel, J. and N. Bose, "Target in \$39.4 Million Settlement with Banks over Data Breach," Reuters (2 December 2015) – <https://www.reuters.com/article/us-target-breach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203>.
19. Target Corporation Customer Data Security Breach Litigation, 2015 – <https://targetbreachsettlement.com/Portals/0/Documents/Settlement%20Agreement.pdf>.
20. Target Corporation, "Target Corporation 10-K for the Fiscal Year Ended January 30, 2016," Target (11 March 2016) – <https://www.sec.gov/Archives/edgar/data/27419/000002741916000043/tgt-20160130x10k.htm>.
21. US Congress. House. Committee on Small Business, Protecting Small Businesses from Cyber Attacks : The cybersecurity Insurance Option : Hearing before the Committee on

Small Business, United States House of Representatives, One Hundred Fifteenth Congress, first session, 2017.

22. Webb, T., "Analyst Sees Target Data Breach Costs Topping \$1 Billion," Twin Cities (January 29, 2014) – <https://www.twincities.com/2014/01/29/analyst-sees-target-data-breach-costs-topping-1-billion/>.
23. Yang, Z. and J. C. Lui , "Security Adoption and Influence of Cyber Insurance Markets in Heterogeneous Networks," Performance Evaluation, pp. 1-17, 5 December 2013.
24. Zaleski, A., "Congress Addresses Cyberwar on Small Business: 14 Million Hacked over Last 12 Months," CNBC (April 5, 2017) – <https://www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html>.

About the Author

Kevin Sesock is a graduate student at Oklahoma State University, currently pursuing his MS in Information Assurance. Kevin serves as the CIO for the Oklahoma Municipal Assurance Group. He was the founding chair of the Oklahoma State advisory subcommittee on web accessibility requirements, a founding officer of the Oklahoma Cybersecurity Coalition, and serves as an officer of the Oklahoma Government IT Association. He may be reached at ksesock@omag.org.



Cyber Risk Is Business Risk

Continued from [page 10](#)

then we can build the foundation upon which security, business stakeholders, and risk leaders form relationships and muscle memory to continue working together towards stronger alignment on managing risk.

About the Author

Tim Norris is a product and solution strategist where he is focused on helping organizations address the security and risk management challenges that come from digital transformation. At RSA, Tim is focused on cyber-attack risk through research, customer engagement, and analyst relations to validate key learnings and evangelize technology solutions that address both security and business risks. He may be reached at Timothy.Norris@rsa.com.

The Open Forum

The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. Articles should be 700-800 words and include a short bio and photo. Please submit to editor@issa.org.