Lemons and Liability: Cyber Warranties as an Experiment in Software Regulation

Daniel W Woods[†‡]

†Coalition Inc., USA
‡University of Edinburgh, UK

July 26, 2023

Abstract

The US National Cybersecurity Strategy seeks to assign responsibility for securing systems to the "most capable actors", which involves making software vendors liable for security failures. To help inform policy-makers, we present a case-study in which private actors voluntarily accepted liability for security failures. Since 2014, various security vendors announced *cyber warranties* that promise to pay-out to customers if the vendor's product fails to prevent a security incident. Cyber warranties are voluntarily offered by vendors in a bid to re-shape market dynamics and avoid the market for lemons, in which cheap but ineffective security products (lemons) crowd-out effective products (peaches). We study fourteen warranties and three broad lessons emerge; (i) liability is not universally opposed by software vendors and may in fact reward vendors of secure software; (ii) disentangling the cause of a security failure presents a challenge to the functioning of liability regimes; and (iii) there is no universal duty of care that could qualify vendors for a safe harbor. These lessons can help policy-makers in crafting the software liability regimes that incentivize vendors to write secure software.

1 Introduction

Holding software vendors liable for bugs and security failures is a perennial public policy proposal [1, 2, 3, 4]. Building on these ideas, the 2023 US National Cybersecurity Strategy notes that "too many vendors ignore best practices" and proposes that policy should "shift liability onto those entities that fail to take reasonable precautions to secure their software". The argument goes that buyers of software struggle to evaluate software security [5] and that vendors are best placed to secure it.

Although liability makes sense in the abstract, it is unclear how policy-makers should design the software liability regime. Notably, former officials said

that "establishing liability for software manufacturers was the most significant—if hardest to achieve—element of the strategy" [6]. This creates a chicken-and-egg problem in that there is no existing experience and wisdom from designing liability regimes, leading to a hesitation in creating regimes that would generate experience and wisdom.

Our paper takes a novel approach in looking to the private sector, which has been voluntarily re-assigning liability for cybersecurity failures since 2014 via *cyber warranties*. Cyber warranties enable the vendor to voluntarily accept (some of) the consequences of cyber incidents that the vendor's product failed to prevent. As a result, the "most capable and best-positioned actors" accept some of the liability for security failures. Thus, cyber warranties represent a free-market experiment in software liability.

The core lesson is that software liability will have a differential impact on the software industry with vendors of secure software the relative winners. For example, our empirical test shows that warranties are offered by vendors with higher quality products as measured by product reviews. Such vendors are less impacted by mandatory liability, given some amount was voluntarily accepted.

Section 2 introduces the case-study of cyber warranties, identifying 14 warranties and tracking the development of this aspect of the market. Section 3 reflects on how this informs potential software liability regimes. Section 4 offers a conclusion.

2 Cyber Warranties

Cyber warranties and software liability have a similar effect in that liability for security failures is shifted to software vendors. However, warranty enthusiasts introduce a novel consideration. Liability regimes not only punish the vendors of insecure products but, in doing so, also reward the vendors of secure products. This idea is an important counter-point to the argument that software liability will destroy markets. To the contrary, market actors voluntarily accepted liability in a bid to re-shape the market in a way that rewards vendors of effective products.

2.1 Case-Study

To see this, we need to go back to the first cyber warranty, announced at Black-Hat USA in 2014. Jeremiah Grossman sketched how the warranty worked:

> *"if a WhiteHat customer is hacked, WhiteHat would refund the customer's money for the services they paid for and the first $250,000 of any breach-related costs." [7]*

At RSA 2015 a few months later, the maximum pay-out was increased to $500k. In an op ed, Grossman argued that warranties could result in "no more snake oil", a pejorative phrase used to describe ineffective InfoSec products [8].

ID	Vendor	Type	Year	Limit*
W1a [7]	WhiteHatSecurity	Security audit	2014	$250k
W1b [7]	WhiteHatSecurity	Security audit	2015	$500k
W2 [11]	SentinelOne	End-point	2016	$1m
W3 [12]	MyDigitalShield	Network	2016	$50k
W4 [13]	Cymmetria	Deception	2016	$1m
W5 [14]	AsTech	Security audit	2017	$5m
W6 [15]	CrowdStrike	End-point	2018	$1m
W7 [16]	Cybereason	End-point	2020	$1m
W8 [17]	ThreatAdvice	MSP	2020	$250k
W9 [18]	Deep Instinct	End-point	2021	$3m
W10 [19]	Rubrik	Back-up	2021	$5m
W11 [20]	Arctic Wolf	SOC	2021	$1m
W12 [21]	Sophos	End-point	2022	$1m
W13 [22]	Kroll	End-point	2022	$1m
W14 [23]	Veeam	Back-up	2023	$5m

Table 1: Publicly announced cyber warranties. * Many of these warranties have additional conditions (e.g. $1k per machine up to a limit of $1m) that reduce the effective limits, although this is not consistently reported.

The argument can be explained with economic theory, namely the "market for lemons" for which George Akerlof won a nobel prize [9]. InfoSec products are credence goods, which means buyers cannot observe effectiveness until after purchase. This can lead to a lemons market, in which low-quality products (lemons) dominate the market because buyers cannot identify higher-quality products (peaches) that are more costly to produce. Warranties change this equilibrium by creating a signal that is more expensive for vendors selling lemons, who must pay out more often because the product fails to stop attacks [10]. In this way, buyers can avoid "snake oil" [8] by purchasing from vendors who offer warranties. Such vendors are accountable for security failures and so more likely to build high-quality products (peaches).

Theory slowly became practice as others vendors announced warranties. Table 1 shows that a further thirteen warranties were announced following WhiteHat's warranty in 2014. Potential pay-outs also grew over time from $250k to up to $5 million for some warranties. Warranties were more common in certain market segments, especially end-point protection.

The proliferation of warranties creates the potential for an empirical test of the signaling value. We collected 13.6k ratings from buyers of 31 "Endpoint Protection Platform" products as classified by Gartner, of which five (a total of 3.1k ratings) were sold with a cyber warranty. The vendors who announced cyber warranties occupy position 4 (Sophos), 6 (SentinelOne), 7 (CrowdStrike), 18 (Cybereason) and 29 (Deep Instinct) if we use the number of ratings as a proxy for market size.

The mean rating (from one to five stars) for vendors offering warranties was 4.81 compared to 4.46 for the others. Both sub-samples have a median rating of 5 stars. The volume of observations ($n = 13.6k$) means the difference between

these two means is statistically significant on most tests (e.g. the Mann-Whitney U test: (U = 20.7m, $p < 0.0001$).

This observational evidence shows that products offered with a warranty achieve higher customer satisfaction. This supports the prediction from economic theory that warranties would be offered by vendors to signal higher quality goods [9, 10]. Admittedly, ratings capture more than simply how effective the product is at preventing attacks, which is difficult for buyers to evaluate even after installing the product. Ratings also capture factors beyond core functionality, such as customer service.

This story should be qualified by critiques of the terms and conditions of cyber warranties. In particular, vendors only cover specific costs related to the functionality of the vendor's product. A software auditing vendor's warranty (W5) only covers losses resulting from vulnerabilities that were publicly known at the time of the audit [24]. Similarly, a back-up providers only covers ransom demands that are offered in exchange for the cryptographic key that can recover systems [25]. The warranty does not cover ransoms demanded under the threat of leaking personal data, which is understandable given back-ups do not protect the confidentiality of data.

3 Implications

This raises the question of what lessons can be learned for software liability set by governments. Cyber warranties flip the conventional wisdom on software liability. In the past, proposals were held back by fears that liability would stifle innovation [6]. If this was universally true, it is unclear why the security vendors in our case-study voluntarily accepted liability via warranties.

An alternative interpretation is that the status quo of no liability stifles the production of secure software. Vendors skimp on investing in secure software because buyers cannot easily discern secure from insecure [26], which means the market does not reward the investment. This leads to a 'market for lemons', in the language of Akerlof [9], to the benefit of vendors of insecure software. Our case study shows that transferring a small amount of liability—voluntarily accepted by the vendor offering the warranty—helps to address the market for lemons. This raises the question of whether more liability transfer is necessarily better, or whether voluntary warranties should be left to evolve.

The growth of cyber warranties could be supported by policy makers. This would range from discussing warranties in strategy documents to endorsing products offered with warranties through to incorporating warranty availability into government procurement decisions. This approach requires less political capital, not least because vendors control how much liability they accept. The policy goal would be to establish in a norm in which InfoSec vendors voluntarily offer warranties.

The problem with this approach is that warranties have been so slow to proliferate. Even in the market segment in which warranties are most widespread, namely End-Point Protection, products sold with a warranty represent just

22.8% of product ratings. Warranties are much rarer for other InfoSec segments, and non-existent in the rest. We did not identify any security warranties for non-security software, even though it can also be targeted in security incidents. This all suggests that vendor voluntarily offering warranties will not move the needle, and more drastic measures will be needed to re-assign responsibility at scale.

The contractual wording of warranties highlights a challenge in doing so. Cyber warranties are crafted so that vendors are only liable for failures that the vendor's product was designed to prevent. For example, the back-up provider covered ransom threats based on encrypted systems but not leaked data because back-ups cannot prevent the former. Assigning responsibility to specific vendors may be challenging because DFIR investigations are inconsistent in identifying a singular root cause for cybersecurity failures [27, 28, 29]. This is partly because attacks involve multiple steps exploiting networks of software systems made up of various libraries, micro services and proprietary code. It is also because the legal system creates incentives to obfuscate root causes [30]. The resulting uncertainty will undermine the functioning of the liability regime—warranties get around this by affirmatively stating what will be covered, even though this creates the possibility a victim could receive two warranty payments (e.g. if both warranties are triggered).

Another challenge is to affirmatively define *reasonable care* across different products and services. For example, the software auditing vendor defined their warranty in terms of identifying known CVEs, but this is not relevant for a back-up firm. Policy makers may try to abstract away from this problem by focusing on processes that the vendor follows, such as a secure software development life cycle. But linking a failure back to the implementation of high-level processes will be challenging.

A further cautionary tale can be seen in the warranties requiring that the customer follows steps related to the installation, operation and maintenance of products. Such obligations are in tension with the national cybersecurity strategy's goal of easing the burden on users with "limited resources and competing priorities". Again, we face the problem that this balance will be different depending on context.

4 Conclusion

The first cyber warranty was announced in 2014, which was followed by a further 13 over the next decade. The pace of announcements appears to have accelerated, particularly in the end-point protection market segment. Our empirical test showed that products offered with warranties achieve higher product satisfaction, which suggests that warranties signal some aspect of quality. However, detractors point to the relatively narrow coverage offered.

A decade of cyber warranties points to lessons for policy-makers crafting novel security liability regimes:

1. Liability rewards vendors who create secure software. Without any ac-

countability, those vendors lose market share to vendors selling insecure software (lemons).

2. Warranties take responsibility for a sub-set of security incidents linked to the product's functionality. This results from the complexity of corporate networks, in which assigning one single cause of failure is a hard problem. The associated uncertainty could undermine the efficacy of liability regimes.

3. It is challenging to define what *reasonable care* looks like with regards to building security into software as this varies by product. This necessitates policy measures and legislation that account for context.

While these lessons are not new, the case-study of cyber warranties provides real-world lessons and experiences.

A different lesson is that markets can, in admittedly limited circumstances, establish private institutions that assign liability to software vendors without any impetus from policy makers. This raises an entirely new approach for policy makers, namely supporting vendors in voluntarily offering cyber warranties. Such an approach avoids the painful process of drafting and passing legislation, or creating and clarifying regulatory authority. It is surely worthy of exploration.

References

[1] Michael C Gemignani. Product liability and software. *Rutgers Computer & Tech. Law Journal*, 8:173, 1980.

[2] Ross J Anderson. Liability and computer security: Nine principles. In *European Symp. on Research in Computer Security*, pages 231–245. Springer, 1994.

[3] Daniel J Ryan and C Heckman. Two views on security software liability. let the legal system decide. *IEEE Security & Privacy*, 1(1):70–72, 2003.

[4] Terrence August and Tunay I Tunca. Who should be responsible for software security? a comparative analysis of liability policies in network environments. *Management Science*, 57(5):934–959, 2011.

[5] Ross Anderson. Why information security is hard—An economic perspective. In *Proc. of the Computer Security Applications Conf.*, pages 358–365. IEEE, 2001.

[6] Dustin Volz. Biden National Cyber Strategy Seeks to Hold Software Firms Liable for Insecurity `https://www.wsj.com/articles/biden-national-cyber-strategy-seeks-to-hold-software-firms-liable-for-insecurity-67c592d6`, 2023. [Online; accessed 22-Mar-2023].

[7] Sean Michael Kerner. Whitehat is guaranteeing security. *eWeek*, 2015. Accessed: 2023-02-7.

[8] Jeremiah Grossman. No More Snake Oil: Why InfoSec Needs Security Guarantees Available: `https://www.slideshare.net/jeremiahgrossman/no-more-snake-oil-why-infosec-needs-security-guarantees`, 2015. [Online; accessed 27-Feb-2023].

[9] George A Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. In Peter Diamond and Andrew Rothschild, editors, *Uncertainty in Economics*, pages 235–251. Elsevier, 1978.

[10] Daniel W Woods and Andrew C Simpson. Cyber-warranties as a quality signal for information security products. In *International Conference on Decision and Game Theory for Security*, pages 22–37. Springer, 2018.

[11] Lindsay Ciulla. Sentinelone establishes $1 million cyber threat protection warranty giving first-ever industry assurance against growing threats. https://www.sentinelone.com/press/sentinelone-establishes-1-million-cyber-threat-protection-guarantee/, 2016. Accessed: 2023-02-7.

[12] Robert Byrd and Michiko Morales. Assurant partners with mydigitalshield to offer small businesses protection against data breaches. https://www.assurant.com/newsroom-detail/NewsReleases/2016/June/Assurant-Partners-with-MyDigitalShield-to-Offer-Ticker-Businesses-Protection-against-Data-Breaches, 2016. Accessed: 2023-02-7.

[13] Nathaniel Mott. Cymmetria offers $1m warranty to make cybersecurity more accountable. *Tom's Hardware*, 2016. Accessed: 2023-02-7.

[14] Dark Reading Staff. Astech offers a $5 million security breach warranty. *Dark Reading*, 2017. Accessed: 2023-02-7.

[15] Catalin Cimpanu. Crowdstrike to pay up to $1 million warranty if its clients suffer a data breach. *Bleeping Computer*, 2018. Accessed: 2023-02-7.

[16] Sabina Reghellin. Cybereason announces $1 million comprehensive breach protection warranty. *IT Security Guru*, 2020. Accessed: 2023-02-7.

[17] ThreatAdvice. Threatadvice breach prevention warranty. https://www.threatadvice.com/warranty, 2020. Accessed: 2023-02-7.

[18] Steve Zurier. Deep Instinct to offer $3 million ransomware warranty. *SC Media*, 2021. Accessed: 2023-02-7.

[19] Chris Mellor. Up to $5m compensation if rubrik cloud vault recovery busted. *Blocks & Files*, 2022. Accessed: 2023-02-7.

[20] Arctic Wolf. Arctic wolf backs security operations portfolio with $1 million service assurance benefit. https://arcticwolf.com/resources/press-releases/arctic-wolf-backs-security-operations-portfolio-with-1-million-service-assurance-benefit/, 2021. Accessed: 2023-02-27.

[21] Rob Harrison. Introducing the sophos breach protection warranty. https://news.sophos.com/en-us/2022/11/30/introducing-the-sophos-breach-protection-warranty/, 2022. Accessed: 2023-02-7.

[22] Devonne Cusi and Lindsey Challis. Kroll adds complimentary $1 million incident protection warranty to managed detection and response (mdr) service. *Business Wire*, 2022. Accessed: 2023-02-7.

[23] Veeam. Veeam ransomware recovery warranty veeam has you covered. https://www.veeam.com/products/ransomware-recovery-warranty.html, 2023. Accessed: 2023-02-27.

[24] Daniel W Woods and Tyler Moore. Cyber warranties: market fix or marketing trick? *Communications of the ACM*, 63(4):104–107, 2020.

[25] Rubrik, Inc. Rubrik enterprise edition ransomware recovery warranty agreement. https://www.rubrik.com/content/dam/rubrik/en/resources/policy/rubrik-enterprise-edition-ransomware-recovery-warranty-agreement.pdf, 2022. Accessed: 2023-02-7.

[26] Ross Anderson and Tyler Moore. The economics of information security. *Science*, 314(5799):610–613, 2006.

[27] Martin Gilje Jaatun, Eirik Albrechtsen, Maria B Line, Inger Anne Tøndel, and Odd Helge Longva. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2(1-2):26–37, 2009.

[28] Josephine Wolff. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. MIT Press, 2018.

[29] Rob Knake, Adam Shostack, and Tarah Wheeler. Learning from cyber incidents: Adapting aviation safety models to cybersecurity. *Harvard Belfer Center*, 2021.

[30] Daniel Schwarcz, Josephine Wolff, and Daniel W Woods. How privilege undermines cybersecurity. *Harvard Journal of Law & Technology*, 2023 (forthcoming).