Cyber warranties: market fix or marketing trick?

Daniel W. Woods and Tyler Moore

Abstract

The market for information security products is plagued by information asymmetry, dysfunctional brand reputation and principal-agent problems. Mechanisms to address the resulting market for lemons include certification schemes, liability laws, and information disclosure. Unfortunately there has been limited success thus far. An emerging form of risk transfer, cyber warranties, could address the market failure. We analyse 15 warranties to identify what is covered and what is excluded. The results suggest cyber warranties do not transfer much risk at present. However, they do force transparency regarding the limitations of information security products.

1 Introduction

When buying a second-hand car you are at the mercy of the dealer. The dealer knows which cars were treated well by past owners and which are likely to break down within a few months. When buying an information security product, the vendor has a better idea of how effective the product truly is. In both cases the seller has information the buyer lacks.

Economists refer to this phenomenon as a market with asymmetric information. Akerlof [1] suggested this leads to a "market for lemons" dominated by lower quality goods (aka lemons in the case of used cars). Consumers cannot identify differentiate between lemons and quality-used cars. Akerlof's model suggests only lemons would be sold in such a market.

Car dealers offer warranties to overcome this problem. If the used-car breaks down within, say, six months, the dealer must pay for its repair. This discourages dealers selling lemons from offering lengthy warranties. Consequently, the length of the warranty provides information about how likely the vehicle is to break down.

Returning to information security, vendors have started attaching cyber warranties to information security products with no additional fee. Will cyber warranties better align incentives in the market for information security products?

Accepted for Publication in the Communications of the ACM
DOI: https://doi.org/10.1145/3360310

Or are they marketing tricks riddled with coverage exclusions hidden in the fine print of the terms and conditions?

2 Might cyber warranties remedy the market for lemons?

A natural first question to ask is why warranties might succeed in addressing the market for lemons where other mechanisms have failed. Akerlof [1] identified mechanisms to address this including brand reputation, certification, liability laws, and warranties.

Evaluating the effectiveness of products is difficult because they appear to be working until an attack takes place. Reputation systems are further limited by commercial sensitivity preventing information from being pooled across organisations. Vendors instead signal quality by speaking at conferences, publishing security research, and through marketing activities. The latter can lead to (arguably deceptive) claims about product functionality that may not reflect reality.

External experts could certify the effectiveness of the product. Certification firms face incentives to skimp on assessment. A framework for certifying computer systems as secure "motivated the vendor to shop around for the evaluation contractor who would give his product the easiest ride" [2]. Even if such incentives were overcome, there are difficulties in using laboratory experiments to establish real world security.

Liability laws could shift the costs of an ineffective product back onto the vendor. This might incentivise vendors to create more effective products and even force firms selling ineffective products out of the market. However, the resistance to software liability is well documented [3]. To prove vendors liable for creating a defective product, the product in question must be shown to have caused the injury. Establishing such proximate cause is fiendishly hard, given the constellation of security controls employed by firms.

So why might cyber warranties succeed where other approaches have failed? Certification incurs large up-front costs regardless of effectiveness, whereas warranties only incur a cost when the product fails to mitigate an attack. Consequently, vendors with more effective products incur less cost in offering warranties. Further, barriers to adoption can be overcome by individual firms unilaterally offering warranties—courts need not assign liability nor governments pass legislation.

This article evaluates three viewpoints on the role of warranties. The theoretical view argues cyber warranties can align incentives and fix a dysfunctional market, as put forward in [4]. A skeptical view characterises cyber warranties as marketing tricks offering little meaningful coverage to the buyer. The conciliatory view holds that while warranties do not significantly change the incentive to invest, they do prevent vendors from over-exaggerating the functionality of products. Which viewpoint best describes reality can be answered empirically

by inspecting the terms of the warranties, which we undertake next.

3 What do cyber warranties cover?

We searched for combinations of the terms "warranty", "indemnity", "information", "security", and "cyber" using a popular search engine. We stopped when further results revealed no new warranties attached to information security products. Some vendors provide a description of the warranty without the actual contract, we included these descriptions in our corpus if they were detailed enough for our purposes. This resulted in a corpus of 15 warranties attached to information security products.

Inductive analysis identified *coverage*, *obligations* and *exclusions* as the main components of the warranties. *Coverage* describes which costs the vendor will indemnify and the total indemnification limit. *Obligations* describe what the buyer must do for the warranty to be valid. *Exclusions* describe which circumstances invalidate coverage.

Consumers should first ask whether the product comes with a product or incident warranty. Of the 15 warranties, two thirds were only triggered by defective hardware or software. We will call these *cyber-product warranties* from now on and denote by P in Table 1. Cyber-product warranties offer to repair or replace the product, denying coverage for first- or third-party costs resulting from an attack.

Cyber-incident warranties (denoted by I in Table 1) cover the consequences of an attack. Four of the five cyber-incident warranties in our sample covered first-party costs like notifying customers and hiring consultants for forensic investigation, public relations or legal review. One vendor explicitly covered ransomware payments and nothing else (denoted I^{RWP}). None of the warranties (I or P) cover regulatory fines or third-party liability. The amount of coverage ranged from $10,000 to $5,000,000 depending on the size of the buyer.

Obligations on the buyer can be classified into install-time, ongoing and post-incident. Ongoing and install-time obligations are most common. The majority (denoted V in Table 1) use vague terms like *proper* maintenance and operation without a concrete definition for what this entails. However, some warranties (denoted P) are exceptions in providing prescriptive obligations. These vendors tend to offer higher limits. For example, one vendor requires a "differential security analysis" whenever the buyer modifies software covered by the warranty. Another vendor requires the client to relinquish write access to the product and allow the vendor to configure security functions like the whitelist. Post-incident obligations concern when and how the client must notify the vendor after discovering the incident.

There is significant diversity in terms of what cyber-incident warranties exclude. For example, a back-up provider excludes "any breach due to weak or stolen credentials" or "denial of service". A monitoring product excludes breaches that are "not a result of APT activity". A firm offering source code review excludes coverage if the attack results from unknown vulnerabilities, de-

Description	Contract	Coverage Type	Coverage Amount	Install time	Ongoing	Post-incident
Routers	Y	P	Repair or Replace		V	
Access control	Y	P	Repair or Replace	V	Y	
Security tokens	Y	P	Repair or Replace		P	
Network mgmt	Y	P	Repair or Replace			
End-point protection	Y	P	Repair or Replace	V	Y	
Network architecture	Y	P	Repair or Replace	V	V	
Various products	N	P	Repair or Replace		V	
Firewalls	Y	P	Repair or Replace		V	
Routers	Y	P	Repair or Replace	V	V	
Firewalls	Y	P	Repair or Replace	V	V	
Source code review	Y	I	$5,000,000		V	30 days
Back-up services	Y	I	$10,000/$50,000	V	P	30 days
End-point protection	N	I	$100,000/$500,000 /$1,000,000		P	
Monitoring	Y	I	$1,000,000 or 2x License fee	V	V	
End-point protection	N	I^{RWP}	$1,000,000 or $1,000 per end-point	V	P	

Table 1: Columns refer to: a description of the vendor, whether we have the actual contract (Yes (Y) or No (N)), the type and amount of coverage offered and whether there are obligations (Vague (V) or prescriptive (P)) for install time, ongoing, or post-incident.

fined elaborately using the CVE database and a list of 122 known vulnerabilities.

Consumers might worry about the vendor's ability to fund the indemnity payment. Some cyber-incident warranties were backed by insurance. For example, one vendor claimed to be "underwritten by an A-rated, internationally known insurance carrier". A different vendor suggested their relationship with insurers meant purchasing the product "could result in better terms on cyber insurance".

Our corpus represents close to the population of cyber-incident warranties while only comprising a sample of cyber-product warranties. The latter are predominantly offered by firms selling physical devices to be deployed in the buyer's network. The corresponding warranties are less diverse and less likely to be announced publicly. This can be contrasted with cyber-incident warranties, which are announced publicly to generate coverage from security reporters. Firms offering cyber-incident warranties sell intangible products and services like source code review, network monitoring, or back-up services.

4 Looking forward

Warranties must transfer non-negligible amounts of liability to vendors in order to meaningfully overcome the market for lemons. Our preliminary analysis suggest the majority of cyber warranties cover the cost of repairing the device alone. Only cyber-incident warranties cover first-party costs from cyber attacks.

Consumers should question whether warranties can function as a costly signal when narrow coverage means vendors accept little risk.

Worse still, buyers cannot compare across cyber-incident warranty contracts due to the diversity of obligations and exclusions. Ambiguous definitions of the buyer's obligations and excluded events create uncertainty over what is covered. Moving towards standardised terms and conditions may help consumers, as has been pursued in cyber insurance, but this is difficult for specialised products.

The scope of the product drives warranty terms and conditions. The source code review firm only indemnifying losses resulting from known vulnerabilities with a corresponding CVE number protects the vendor from incurring costs for not anticipating zero-days. But there are less reasonable exclusions like the monitoring firm only indemnifying losses resulting from "APT activity", which is strange since non-APT attacks are presumably easier to detect.

Warranties with many obligations and exclusions at least communicate the attached product's limitations. Prescriptive ongoing obligations from end-point protection firms demonstrate how security is about more than just buying the right product. In fact, the expertise of security professionals is so important that one firm invalidates coverage unless the buyer relinquishes write access to the platform.

Theoretical work [4] suggests both the breadth of the warranty and the price of a product determine whether the warranty functions as a quality signal. Our analysis has not touched upon the price of these products. It could be that firms with ineffective products pass the cost of the warranty on to buyers via higher prices. Future studies could analyse warranties and price together to probe this issue.

To conclude, cyber warranties—particularly cyber-product warranties—do not transfer enough risk to be a market fix as imagined in [4]. But this does not mean they are pure marketing tricks either. The most valuable, albeit underappreciated, feature of warranties is in preventing vendors from exaggerating what their products can do. Consumers who read the fine print can place greater trust in marketing claims so long as the functionality is covered by a cyber-incident warranty.

Acknowledgements

The collaboration was made possible by a Fulbright Cybersecurity Scholar award from the US-UK Fulbright Commission.

References

[1] 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.

[2] Ross Anderson. Why information security is hard-an economic perspective. In *Proceedings of the 17th Annual Computer Security Applications Conference*, pages 358–365. IEEE, 2001.

[3] Michael L Rustad and Thomas H Koenig. The tort of negligent enablement of cybercrime. *Berkeley Tech. LJ*, 20:1553, 2005.

[4] Daniel W Woods and Andrew C Simpson. Cyber-warranties as a quality signal for information security products. In *Proceedings of the 9th Conference on Decision and Game Theory for Security*, pages 22–37. Springer, 2018.