SAFER CYBERSECURITY BUYERS' CHARTER

Fundamental Principles for SAFER Cybersecurity Purchasing

- answering the question "what does this do?"

Published: May 2021

Fundamental Principles for SAFER Cybersecurity Purchasing *- answering the question "what does this do?"*

We, as a community, want to see secure, prosperous and open digital societies. A secure digital environment is in our interests. Yet currently, that environment has too many structural insecurities, one being the continued failures in cybersecurity. This charter builds on the conclusions from the 2020 Debate Security report on cybersecurity technology efficacy[1], which clarified some of the structural problems hindering us from tackling cybersecurity effectively:

- **Lack of transparency:** too often, those who want to do the right thing and protect their assets don't have the right information to evaluate cybersecurity solutions;
- **Excessive noise:** those with innovative cybersecurity solutions to sell can't break through amidst the noise of the market; and
- **Perverse incentives:** current market incentives encourage cybersecurity vendors to focus on speed to market rather than security performance.

This is a market problem. It is best solved by free market solutions. We therefore want to improve the functioning of a free market in the public interest. As vendors, buyers and key members of the ecosystem alike, we want to work together to make this happen.

We support the SAFER Buyers' Charter to incentivise more effective cybersecurity.

1 https://www.debatesecurity.com/cybersecurity-technology-efficacy-is-cybersecurity-the-new-market-for-lemons/

Through this Charter, we commit together to developing the Fundamental Principles for SAFER Cybersecurity Buying, through:

S	A	F	E	R
Symmetry of information between buyer and vendor, addressing the fundamental imbalance at the root of the problem;	**Assessment** independence and approach which make it easier for vendors with effective solutions to navigate markets successfully and for buyers to access independent assurance;	**Freedom** of entry and innovation in the market, maintaining, as far as possible, low barriers to new entrants with demonstrably effective solutions;	**Efficacy-based assurance,** ensuring that assessors look at the total efficacy of a solution when assuring or reviewing cybersecurity solutions;	**Risk-based buying decisions,** providing buyers with solution efficacy information to drive a value-based buying decision, trading off likely risk reduction with cost.

All of this is underpinned by a commitment from buyers and vendors alike to conduct business in plain, understandable language. When it comes to a cybersecurity product or service, vendor and buyer alike must be able to explain clearly.

What does this do?

We undertake to work together with all parties to develop solutions and drive implementation of these principles. This undertaking is outlined by the commitments we make in this charter.

In the following sections we review each of the SAFER principles to highlight the issue, relevance, possibilities for action, impact of succeeding and risks and challenges, and we describe the commitments we will make to implement the principles. These form the starting point for working together to develop the detailed arrangements required to implement the SAFER principles.

Symmetry of information

Objective
Achieve symmetry of information between buyer and vendor, addressing the fundamental imbalance at the root of the problem.

The issue
At present, there is a fundamental imbalance between the information available to vendors, who have full access to information about their product, and buyers, who don't. As a result, buyers who don't have deep technical assurance capabilities within their own organisation risk buying cybersecurity solutions that are not fit for purpose and therefore will be ineffective to address their needs. From the vendor side, the current market incentives mean that there is a first-mover disadvantage to overcome with regards to investment in greater efficacy. Until those incentives are addressed, and buyers demand better transparency on efficacy, it is not in their interest to address the imbalance.

The relevance
This is one of the most fundamental problems in cybersecurity. We are now past the age of 'awareness raising': all responsible organisations should be aware of the cyber risk. But how does a responsible executive know what to buy?

The possibilities for action
Whilst many of the recommendations in this charter are specific changes to procedures and practice, this one is also cultural and behavioural, and critically, it is fundamental to all other aspects of the charter. Better assessment frameworks, freedom of market entry, efficacy-based assurance, and risk-based buying all spring from a new approach to buying cybersecurity based on asking – and understanding – the question "what does this do" when considering a cybersecurity solution.

There must be a minimum expectation in the industry that when buying a solution:

- its technical components can be explained clearly,
- it can be related to the business need of the buying organisation, and
- there is clarity on how it will help manage risk and lower the probability of harm.

The products or services bought can then form a part of a coherent risk reduction strategy.

The impact of succeeding
Creating greater transparency in the buying process for cybersecurity solutions could be transformative. Giving the best available knowledge to operational decision-makers will enable them to move to more risk-based decision making and better evaluation of their options.

The risks and challenges
Cultural changes are hard to deliver: this cannot be legislated or wished into existence. It requires training, awareness raising, education and a willingness, in particular from buyers, to know how to ask the right questions and be prepared to do so. Until there is a radical shift in the industry, buyers will need to demand new levels of transparency to ensure that the incentives are there for the vendors to improve.

Assessment independence and approach

Objective
Establish independence and an approach for assessment which make it easier for vendors with effective solutions to navigate markets successfully and for buyers to access independent assurance;

The issue
The 'business of reviews' and the 'power of marketing' strongly affect the market today. Buyers are offered myriad product reviews that typically don't show the full picture of a solution's efficacy. The reality of cybersecurity technology is that it is complex, yet the information asymmetry outlined above means that buyers must rely on reviews and marketing to make buying decisions. Current assessments such as the MITRE ATT&CK framework have shown that the efficacy of a solution is often context and threat dependent, making it incredibly difficult to fully assess a solution, and current commercial incentives mean ensuring independence of reviews is increasingly challenging.

The relevance
Without independent efficacy assessment, buyers cannot gain full access to unbiased, complete information about the solutions they are buying and the market failings will continue. The complexity of today's solutions means that the market needs a functioning assessment capability to reduce the dependency on external inputs when selecting solutions.

The possibilities for action
There are various ways in which new frameworks could be developed for independent assessment of cybersecurity solutions. One possible approach to ensure independent assessment without sacrificing innovation would be to define standards based on assessment and/or outcomes rather than technology. Assessment standards would describe the methodology that should be used to assess a technology rather than describing how the technology should be designed or configured, thus avoiding stifling innovation. Assessment standards could be designed to cover the required outcomes and relevant input factors of a solution. In a market where private bodies undertake assessments, regulators could inspect the assessors to make sure they have the required abilities, independence and track record of working to the standard.

The impact of succeeding
If we get assessments right, buyers will be able to make fully risk-informed decisions. Additionally, it will become easier for good products and services to shine through, incentivising investment in efficacy over marketing.

The risks and challenges
Details matter. Getting an assessments framework wrong could lead both to poorer outcomes, and a loss of confidence in the system. Equally, standards would need to be international to cater for global organisations and avoid a proliferation of standards. Finally, assessors would need to be given appropriate legal protections to avoid constant litigation in response to their assessments.

Free-market access

Objective
Freedom of entry and innovation in the market, maintaining, as far as possible, low barriers to new entrants with demonstrably effective solutions;

The issue
Current low barriers to entry enable a huge amount of innovation but with no efficacy measurement the market has become noisy and makes it increasingly difficult for high efficacy solutions to shine through.

The relevance
The cybersecurity market has relatively low barriers to entry today, as vendors are able to sell without structured market evaluation in many commercial markets. The market incentives today encourage new entrants to focus on speed to market and marketing spend rather than efficacy.

The possibilities for action
Imposing standards on assessment rather than on the technology, as outlined above, would limit the risk of innovation being stifled by needing to conform to standards. Freedom to enter can also be maintained by aligning efficacy assessments to the scale and type of business that is bringing the new (or updated) solution to market. In terms of scale, the depth of assessment that is expected could be moderated, a greater depth of assessment would be expected for solutions from larger organisations and more shallow assessment for smaller, less complex, new entrants. For example, the level of assessment required for a hugely complex global technology would be more complex and broad than of a boot-strapping start-up, and the cost of assessment could align to the scale. This would clearly create a difference in risk profile between the largest and the smallest vendors, however, this difference is accepted today even without the SAFER principles; the assessment is merely formalising it.

The impact of succeeding
If freedom to enter and innovate is maintained, the market can continue to evolve in line with buyer needs and technical advancement. Independent assessment can help support freedom of entry and innovation because it allows new entrants to focus on developing good solutions that do well in assessment rather than focusing on marketing to cut through the noisy marketplace. Fixing the market failing will allow high-efficacy, moderately-funded innovation to succeed over low-efficacy, well-funded alternatives, thus improving market freedoms.

The risks and challenges
Freedom to enter could be at risk if the measures imposed to raise the efficacy bar are biased towards incumbents and create barriers to entry that are prohibitively expensive for new players. Limiting freedom to enter in this way would mean that buyers no longer have access to the most innovative solutions as it would be too expensive and complicated to develop them. Additionally, freedom to innovate could be at risk if standards are excessively prescriptive in terms of technology architectures and performance requirements. There is great concern in the vendor community that technology standards by definition impact the ability for them to innovate.

Efficacy-based assurance

Objective
Use efficacy-based assurance, ensuring that assessors look at the total efficacy of a solution when assuring or reviewing cybersecurity solutions. Efficacy is defined by[2].

- Capability to deliver the security mission (fit-for-purpose); ie. how well does this solution create the outcomes claimed by the vendor?
- Practicality in operations (fit-for-use); ie. how easy is this solution to integrate and use within an enterprise environment?
- Quality of security build and architecture; ie. how securely has this solution been built, how many build errors were found?
- Provenance of the vendor and supply chain; ie. how secure is the vendor organisation providing the solution, how much vulnerability is there in their supply chain?

The issue
Current efficacy assessments in the market are either:

- too technical to be useful for the general market,
- too narrow as they only focus on one dimension of efficacy,
- too simplistic in their judgement so don't allow a risk-based buying decision.

The dominant assessment organisations typically only look at Capability, meaning buyers do not have a full appreciation of how solutions will reduce cybersecurity risk.

The relevance
Assessing the efficacy of cybersecurity solutions needs to be done in a way that gives buyers real insight into whether or not the solution will meet their needs, and be sustainable over time (given cybersecurity typically has a 'shelf-life' based on the amount of attention it gets from attackers). If the assessment doesn't comprehensively cover the efficacy of the solution then buyers are unable to make fully-informed, risk-based, buying decisions.

[2] *https://www.debatesecurity.com/cybersecurity-technology-efficacy-is-cybersecurity-the-new-market-for-lemons/*

The possibilities for action
Capability can be measured against the vendors claims and a transparent review of the solution design (which clearly will need careful execution to avoid risk of intellectual property loss for vendors). Practicality can be measured in terms of deployment, operational and maintenance effort in a number of clearly defined standard operating environments (potentially according to the assessment organisation), while this doesn't perfectly replicate the buyer environment it at least allows some level of risk-based comparison. Quality can be measured against the discovery of vulnerabilities and errors in build, as well as consideration of vendor quality practices (eg. ISO). Provenance can be measured in terms of the security standards of the supplier and the chain behind it.

The impact of succeeding
If efficacy-based assurance is used in the market then customers will be given more of the information they need to evaluate purchases. Organisations will be better able to integrate solutions into operations (because there will be clearer information about them) and their assurance processes will be better able to evaluate how the company is defending itself. Vendors will have incentives that are more effectively aligned with customer needs and will compete with each other on clearer terms, and finally, regulators will be better able to set assessment standards.

The risks and challenges
The risk with efficacy-based assurance is that it places a greater demand on vendors when they bring products to market, thereby potentially raising the cost of entry significantly

Risk-based decision making

Objective
Support risk-based buying decisions, providing buyers with solution efficacy information to drive a value-based buying decision, trading off likely risk reduction with cost.

The issue
The fundamental problem with today's broken market is that it does not allow buyers to make buying decisions based on risk. Without a clear risk-based view in buying decisions, the market incentives don't align to encourage vendors to create high-efficacy solutions. This means organisations end up with less-effective solutions, potentially exposing themselves to greater risk and incurring more cost in the long-term. Current buying decision-making tends to look for 'tick-box' solutions that meet a simple set of criteria (with a strong focus on up-front costs) rather than considering all the factors that will impact buyer value.

The relevance
Cybersecurity technology efficacy is complex and isn't merely a question of which solution has the most features or which is 'best value' in a category. Buyers today don't have the information they need to be fully aware of the balance of risks with each solution they are evaluating.

The possibilities for action

All of the SAFER elements discussed above demonstrate a clear need for - and path towards - true risk-based buying in cybersecurity. If the most senior members of the buying community (ie. company leaders) demand that their organisations demonstrate the risk-based buying decisions they have made then the practice will develop. Risk-based buying decisions can be enabled by implementing the principles outlined above – placing greater emphasis on transparency of solution efficacy and by developing the skills to evaluate complex solutions. This will require real investment to improve the understanding amongst the buying community of how to evaluate cybersecurity solution assessment reports, and how to trade-off the various risks.

The impact of succeeding

If buying decisions are based on the balanced view of risk for each solution then organisations will be able to better understand the 'return on investment' of one solution versus another. As buyers use this approach it will incentivise vendors to develop solutions that are more effective at reducing risk. It is important to note that this approach also allows buyers to consciously decide to take the risk of buying a lower-efficacy solution for good business reasons (eg. cost, ease of implementation).

The risks and challenges

The risk of implementing this approach too rigorously is 'analysis paralysis' and excessive complexity in buying that reduces the pace of progress. It will be important to avoid reports becoming unreadable to the point that buyers can't use them and revert to reading marketing material to make judgments. Reports will need to be technically authoritative without demanding that buyers have the same level of expertise.

THE COMMITMENTS

The signatories of this SAFER Cybersecurity Buyers' Charter commit to working together with all parties to develop solutions and drive implementation of these principles.

The implementation path is based on three stages, and we expect this to be a 3 to 5 year journey. Stage one will define the requirements from a buyer perspective for a future market model. Stage two would then design new processes and organisations based on the requirements. Then finally, stage three would be the execution of the design, either via new, or within current, organisations.

Commitments are made in the following ways:

As a Leader: joining the Steering Group of the Coalition delivering the Charter.

- The Steering Group will meet quarterly to work on delivering an approach, actionable by industry, that enables the implementation of the principles of the SAFER Cybersecurity Charter.
- Members of the committee will help guide the strategic direction of the work and drive the growth of the coalition.
- Commitment as a leader will include a time commitment to participate in the periodic Steering Group meetings and from the organisation to drive change via working group meetings and market engagement, there is also a financial commitment to support the Coalition.

As a Member: joining the working groups of the Coalition delivering the Charter.

- This includes a time commitment to participate in the working group meetings of the Coalition and a financial commitment to support the Coalition.

As a Supporter on an individual or corporate basis:

- As a commercial organisation, by providing financial support to the Coalition delivering the Charter.
- As a thinktank, academic, or subject matter expert by offering expert thinking and support to amplify the message.