

**DEBATE
SECURITY**

RESEARCH REPORT

CYBERSECURITY TECHNOLOGY EFFICACY

Is cybersecurity the new “market for lemons”?

Reporting findings from interviews
with more than 100 business and
cybersecurity leaders.

Published: October 2020

Contents

Executive Summary	3	Assessment standards and organizations	43
1 Cybersecurity technology has significant efficacy issues	5	Better buying	49
Historical market context	6	Vendor perspective	50
Cybersecurity is failing because the technology is not as effective as it needs to be	7	4 Changing market incentives will require concerted effort on the buy-side	52
Cybersecurity technology efficacy can be defined by four characteristics	8	Proposal for buyers (including all in the enterprise, eg, CISOs, CIO, procurement etc.)	53
Efficacy issues result from myriad vulnerabilities	10	Proposal for vendors	54
2 The underlying problem is one of economics, not technology	11	Proposal for assessors	55
The information asymmetry	12	Proposal for regulators	56
System dynamics and incentives	13	5 Research Methodology	57
Stakeholder views	15	Interviews	58
Enterprise CISO/Buyer – ‘the customer’	16	Cohort	58
Enterprise Leadership	19	Review	58
Vendors and intermediaries	20	Acknowledgments	59
Attacker	24		
Regulator	25		
Buying processes	29		
The resultant market breakdown	33		
3 Independent transparent technology assessment is the solution	37		
The new model	38		
The benefits of the new model	41		
Open issues	42		



Executive Summary

1 Cybersecurity is failing because the technology is not as effective as it needs to be

Cybersecurity is failing. Spend on cybersecurity is increasing every year (+58% over the past five years¹), yet as the WEF has highlighted², business leaders still identify disruption from cyberattack as one of the top 5 growing risks in 2020 (and while the exact numbers are contestable, the direction is clear). A major cause of this failure is that the technology is not as effective as it needs to be, and this is the view shared by 90% of over 100 highly qualified research participants in this study. While there has been a strong focus on improving people and process related issues in recent years, - which are also undoubtedly contributors to cybersecurity failings - technology problems have in some way been accepted as inevitable and the norm. As one Chief Information Security Officer (CISO) put it, “we buy it, and then we cross our fingers and hope the technology will work”. Trust in cybersecurity technology to deliver on its promise is low. Without improving technology efficacy, cybersecurity will continue to fail.

Participants in this research broadly agree that four characteristics are required to comprehensively define cybersecurity technology efficacy. These are the **Capability** to deliver the security mission (fit-for-purpose), **Practicality** in operations (fit-for-use), **Quality** of security build and architecture, and **Provenance** of the vendor and supply chain.

2 The underlying problem is economics, not technology

The root of the efficacy problem is primarily economic rather than technical, characterized by a breakdown in the market relationship between buyers and vendors (‘buyers’ includes CISOs and the broader enterprise team, not only procurement). The core breakdown is an information asymmetry between the parties that prevents buyers from effectively evaluating technology and incentivizes vendors to bring sub-optimal solutions to the market. This mis-match results in products coming to market that are not as effective as promised and which reduce trust in cybersecurity technology. Broken markets have been studied, and solved, before, as evidenced by Akerlof’s 1970 paper ‘Market for Lemons: quality, uncertainty and the market mechanism’. This new research builds on Akerlof’s work and provides the evidence for the breakdown in the market by looking at the overall system dynamics, stakeholder perspectives, buying practices, technology, and vendor landscape; all based on deep interviews and discussion sessions with expert practitioners.

3 Independent transparent technology assessment is proposed as the likely solution

Solving the economic problem requires a new model, creating new incentives for vendors and new approaches for customers. Around 2/3 of the research participants proposed independent and transparent efficacy assessment of technology as the way to solve the information asymmetry, and to rebuild customer trust in the solutions.

¹ <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>

² <http://reports.weforum.org/global-risks-report-2020/appendix-b-methodology/>

Independent and transparent efficacy assessment would give customers better information to make risk-based purchasing decisions and would give vendors stronger incentives to deliver technology with greater efficacy. Over time, improved technology would clearly reduce the likelihood of successful attacks and would have the additional benefit of reducing dependency on people and process (so potentially also reducing the talent gap in cybersecurity). From a vendor perspective, efficacy transparency could help innovation penetrate the market, reducing the need to spend excessively on marketing and sales to gain traction.

For efficacy assessment to keep up with and support technology innovation, market standards should be set for assessment rather than technology. Assessment, rather than technology, standards already exist in some markets and in parts of security today (eg, GSMA NESAS), however, they are not widely understood or used outside these areas.

4 Changing market incentives will require concerted effort on the buy-side

Delivering a new model will require coordinated action on the part of buyers to change the market incentives by demanding efficacy transparency before they trust technology. This approach should remove the first mover disadvantage and unlock the situation. Clearly vendors, assessors and standards setters (typically industry associations or regulators) will also need to play their part in delivering the change, but if buyers create the demand the incentive will exist to do so. The idea of independent transparent technology assessment is not new, but there is little incentive for it in the commercial market today: this study suggests that the time may be right to revisit how this can work. The findings of this work may prompt new questions and debates within organizations and the wider market, some of which will be challenging discussions given the issues identified. However, every effort has been made to give a fair representation of the cohort's views and the intention of this report is to be a catalyst for improvement of the industry and better outcomes for all parties.

5 Research methodology

The perspectives shared in this research have been developed based on 100+ deep interviews with CISOs (representing around 50% of the whole group and coming from globally leading institutions, Fortune 500 companies and elite government environments), cybersecurity vendors, technology vendors, enterprise leaders (Chairs / CEOs), assessment organizations, government agencies and industry associations or regulators. All interviews were conducted on a confidential and non-attributable basis (encouraging candid responses) in between April and September. The interviewees were asked open questions to avoid bias. The author of this research is Joseph Hubback (working as an independent consultant) and it is published by Debate Security, an independent group that brings together industry experts to talk about the cyber market and how it can be improved. Garrison Technology funded Hubback's time while all interviewees contributed on a voluntary basis.



1

CYBERSECURITY TECHNOLOGY HAS SIGNIFICANT EFFICACY ISSUES

Cybersecurity is failing. Spend on cybersecurity is increasing every year (+58% over the past five years³), as the WEF has highlighted⁴, business leaders still identify disruption from cyberattack as one of the top 5 growing risks in 2020 (while the exact numbers are contestable the direction is clear). A major cause of this failure is that the technology is not as effective as it needs to be, and this is the view shared by 90% of 100+ highly qualified research participants in this study. While there has been a strong focus on improving people and process related issues in recent years, - which are also undoubtedly contributors to cybersecurity failings - technology problems have in some way been accepted as inevitable and the norm. As one Chief Information Security Officer (CISO) put it, “we buy it, and then we cross our fingers and hope the technology will work”. Trust in cybersecurity technology to deliver on its promise is low. Without improving technology efficacy, cybersecurity will continue to fail. These findings hold for both independent security technologies and for security functionality embedded in other IT solutions.

Participants in this research broadly agree that four characteristics are required to comprehensively define cybersecurity technology efficacy. These are the **Capability** to deliver the security mission (fit-for-purpose), **Practicality** in operations (fit-for-use), **Quality** of security build and architecture, and **Provenance** of the vendor and supply chain.



CAPABILITY



PRACTICALITY



QUALITY



PROVENANCE

³ <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>

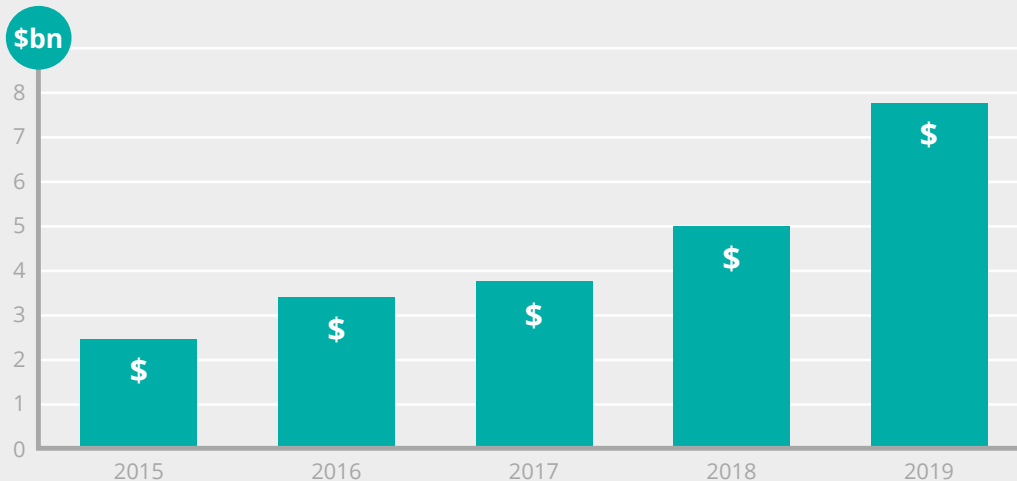
⁴ <http://reports.weforum.org/global-risks-report-2020/appendix-b-methodology/>

Historical market context

The issue of cybersecurity is not a new one. It has been around since the development of electronic computing, especially in the military and government fields. However, since the 1980s and the development of the first mainstream 'worms' the threat to enterprise and personal technology has grown rapidly. Through the 1990s malware grew to a global scale and private enterprise really woke up to the risk. In this period the first major cybersecurity market surge occurred with the development of anti-virus solutions. During the 2000s the Internet economy took off and instances of malware exploded in both number and distribution. In response, end-point protection, network security and application security were further developed. Then the 2010s were marked by an increase in the sophistication of threat actors (both criminal and state-sponsored) and increasingly serious business impacts resulting from attacks.

In combination with increased computing and analytical methods, this increase in threat level during the 2010s has led to a shift in cybersecurity towards monitoring, detection and response technologies in addition to 'traditional' protection solutions. Over the last 40+ years, awareness and knowledge of cybersecurity has gradually grown in the private sector (with some knowledge transfer coming from government sources), prompting greater demand for solutions and very rapid growth in capital investment in the industry (rising from approximately \$2.5bn in 2015 to \$8bn in 2019⁵).

EXHIBIT 1: GLOBAL CYBERSECURITY INVESTMENT PER YEAR



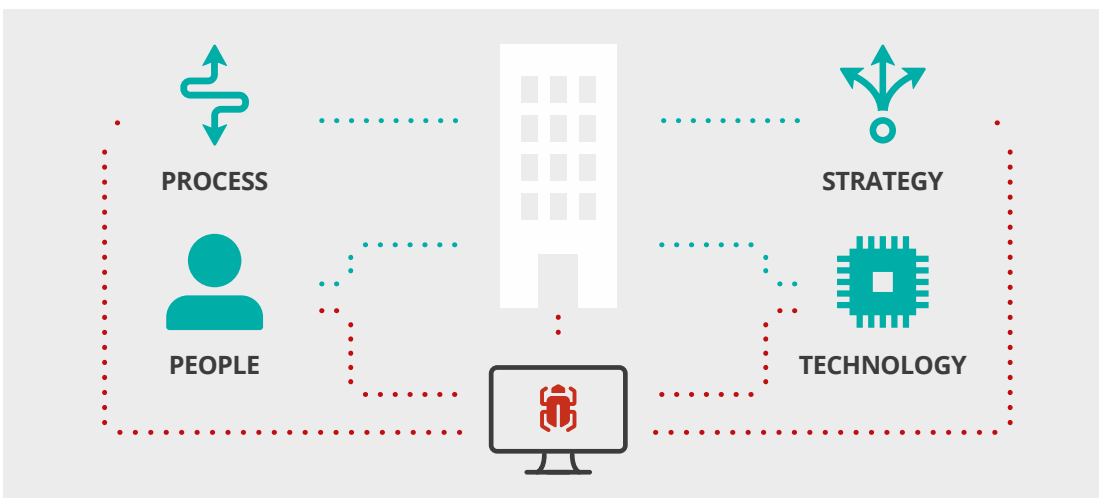
SOURCE: Crunchbase, companies tagged as 'cybersecurity' vs amount raised in the rounds announced in the given year

Cybersecurity is failing because the technology is not as effective as it needs to be

Cybersecurity spending has risen 58% to £121bn over the last 5 years⁶ but this increase in spending hasn't delivered a proportionate decrease in risk. Over the same 5-year period, security breaches have actually increased by 67%⁷, with the damage per victim organization averaging \$13m⁸ and as the WEF has highlighted⁹, business leaders still identify disruption from cyberattack as one of the top 5 growing risks in 2020. As one global bank CISO put it “customers being robbed is becoming normal. Everybody suffers ransomware now; it is also normal. The risk has been accepted.”

Cybersecurity efficacy is dependent on the balance of enterprise defensive and attacker offensive capabilities. It is commonly understood that defensive capabilities are a combination of strategy (what to defend, how to defend; driven by risk governance), process (operational approaches to security), people (security & IT staff, end-users) and technology (hardware and software), as per exhibit 2. Unfortunately, 90% of interviewees in our research say there is an efficacy problem with cybersecurity technology which compromises defences and is partially responsible for the continued success of attackers.

EXHIBIT 2



⁶ <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>

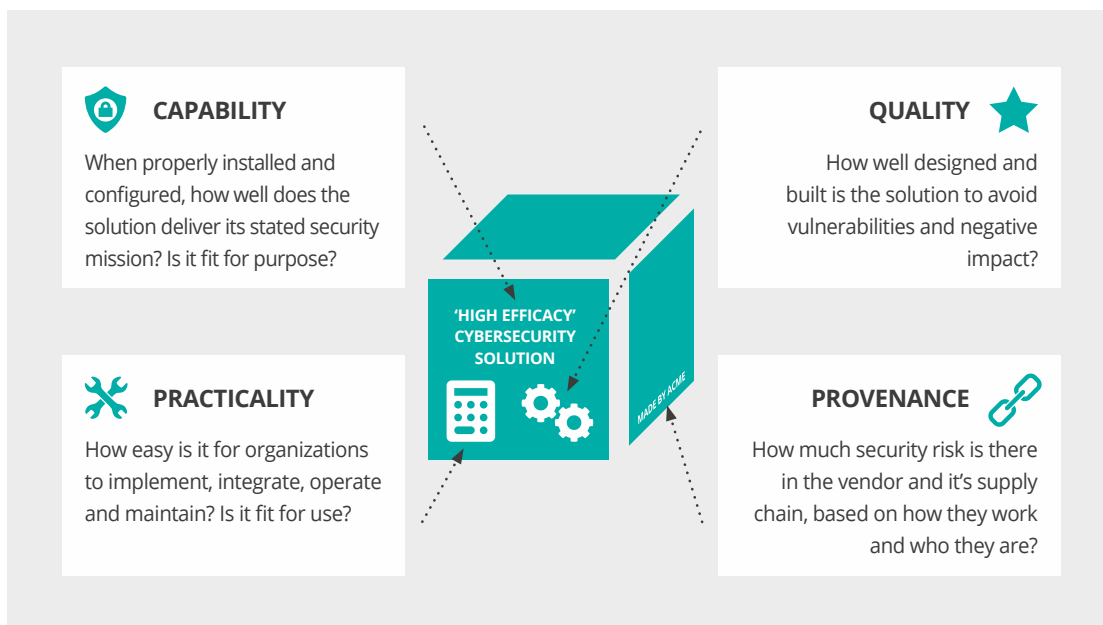
^{7,8} Accentue, Ninth Annual Cost of Cybercrime Study, 2019

⁹ <http://reports.weforum.org/global-risks-report-2020/appendix-b-methodology/>

Cybersecurity technology efficacy can be defined by four characteristics

To be effective, cybersecurity solutions need to have the **Capability** to deliver the stated security mission (be fit-for-purpose), have the **Practicality** that enterprises need to implement, integrate, operate and maintain them (be fit-for-use), have the **Quality** in design and build to avoid vulnerabilities and negative impact, and the **Provenance** in the vendor company, its people and supply chain such that these do not introduce additional security risk.

EXHIBIT 3



This definition of efficacy is not common in the industry and one of the key findings of the research has been the lack of a clear and common definition.

When asked how organizations evaluate cybersecurity technology efficacy, none of the 100+ interviewees referred to a common definition of efficacy. Almost all of them had to take a couple of minutes to structure their thoughts and many of them responded immediately with “wow, that’s a great question, I haven’t thought about that before”. When challenged as to why there is no common view of how to describe cybersecurity technology efficacy the most common response was that most people just ‘accept what we can get’ and ‘have low expectations’, however, the more nuanced view is that it doesn’t exist because most organizations don’t have the capacity to measure it. Some people mentioned a shift in this perspective and that ‘security by design’ was becoming a greater focus, a public example of which could be the AWS Nitro architecture.

The implication of this lack of structured thought about cybersecurity efficacy on the part of customers is that they have been hampered from playing their active role in the market driving up standards and efficacy. The current conventional wisdom in technology markets says it is a ‘fundamental virtue of entrepreneurial innovation’ to bring minimum viable products to market and then to let the market determine future product direction and development. However, this wisdom breaks down in the case of cybersecurity technology because the customers in the market aren’t able to properly assess the solutions delivered and can’t play their role driving the hoped-for direction and development.

When challenged as to why there is no common view of how to describe cybersecurity technology efficacy the most common response was that most people just ‘accept what we can get’ and ‘have low expectations’

Efficacy issues result from myriad vulnerabilities

Cybersecurity attacks can be complex and may exploit multiple vulnerabilities in order to succeed, but attackers are also often opportunistic. The opportunity is based on finding weaknesses in technology and exploiting them before defenders are either aware of them or have had a chance to address them. A lot of focus is placed on the human vulnerabilities that enable successful attacks (such as clicking on links in phishing emails), but this research highlights that technical vulnerabilities due to poor efficacy are also a major contributing factor to successful attacks.

EXHIBIT 4

CORE DESIGN WEAKNESSES



Products with inherent design weaknesses that mean they are less secure than they appear and allow breaches to happen (ie, failing to detect malware), creating a negative impact.

CONFIGURATION COMPLEXITY



Solutions that require excessively complex configuration to deliver the security mission or are by default insecure, meaning excessive risk and driving the high cost of systems administration. Even firewalls can be difficult to configure effectively.

INSECURE ARCHITECTURES



Architectures that are inherently insecure because they rely on functionality that is too complex to deliver security with high levels of assurance.

EXCESSIVE LAYERING



Experience of failures in many and varied solutions mean organizations are pushed to layer multiple different products, leading to excessive cost and poor efficacy (given workload of managing complexity and monitoring alerts).

LACK OF TRANSPARENCY ON SOLUTION CAPABILITY



Many commercial cybersecurity products are not provided with clear information from the vendors of the explicit expected limits of their capabilities, instead they typically over-promise.

SOLUTIONS DIFFICULT TO ASSESS OR AUDIT



Typically a heavy audit workload to understand solution efficacy and also bureaucratic change control processes that reduce agility in assessment. Audits fail to spot poor security given the complexity of the task.

UNDETECTED BREACHES DUE TO DATA COMPLEXITY



Monitoring based on complex multi-dimensional, and often undocumented, data feeds leads to undetected breaches and high workload dealing with false positives. Understanding the data can be very tough.

COSTLY AND TIME-CONSUMING PATCHING



Breaches due to frequent zero-day vulnerabilities in security products (various examples of critical vulnerabilities). High operational demands of keeping security products secure through patching.

EXCESSIVE RELIANCE ON TRAINING



Solutions with weaknesses that make it too easy for human factor errors to enable attacks. We take up users' time with ineffective cybersecurity training (eg, phishing avoidance) and then blame them for breaches.



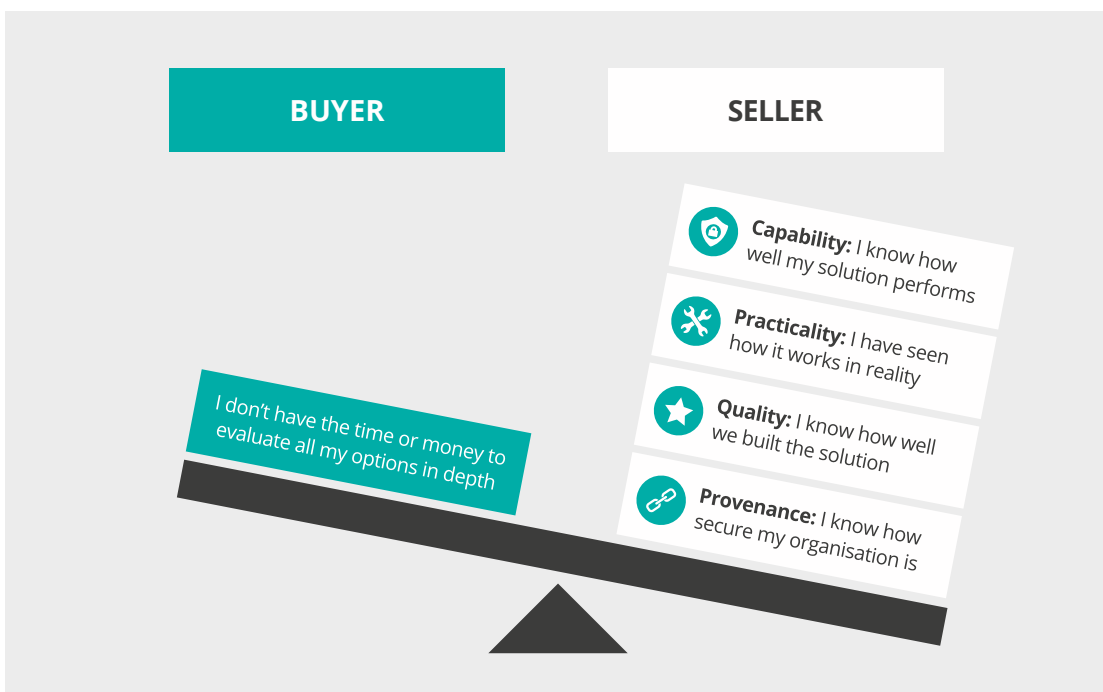
2

THE UNDERLYING PROBLEM IS ONE OF ECONOMICS, NOT TECHNOLOGY

The efficacy problem is the result primarily of an economic not a technological issue, characterized by a breakdown in the market relationship between customers and vendors. When presented with this hypothesis after the open questions in the interviews were completed, all participants who see a problem with technology efficacy agreed and remarked that with the right economic incentives in place they were confident we would see an improvement in technology efficacy. The primary economic breakdown is an information asymmetry that prevents customers from effectively evaluating technology and incentivizes vendors to bring to market solutions which are sub-optimal from a security efficacy perspective. The information asymmetry is demonstrated in in exhibit 5.

The information asymmetry

EXHIBIT 5



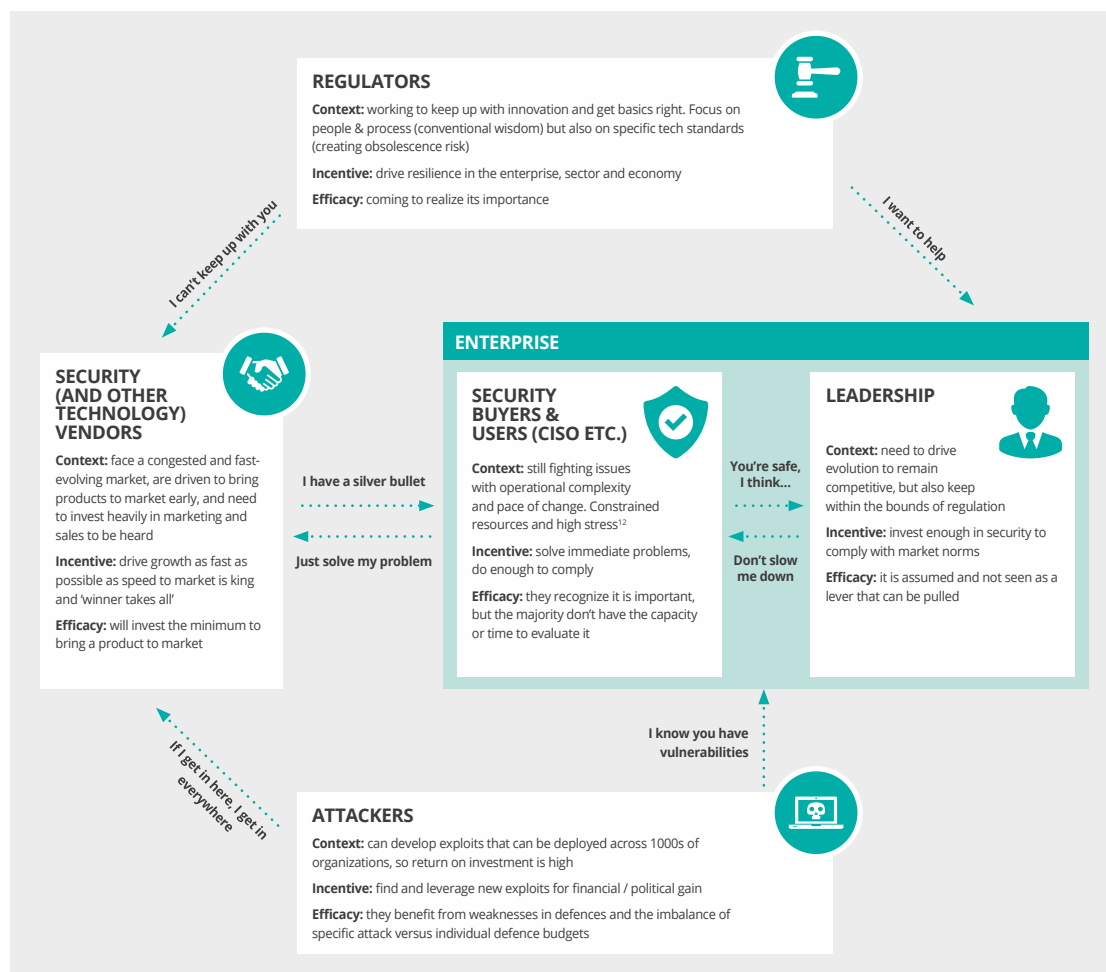
It is worth noting that some might argue there is an information asymmetry working in the opposite direction in that vendors don't have transparency of buyer's needs, however, this is discounted as that information is commonly available and almost always offered if requested.

Broken markets have been studied, and solved, before, as evidenced by Akerlof's 1970 paper 'Market for Lemons: quality uncertainty and the market mechanism'¹⁰. Interestingly, in cybersecurity specifically, market issues are not new. As far back as March 2009 Jim Lewis of the Center for Strategic and International Studies testified to The House Committee on Homeland Security (Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology) about market issues, with his statement saying, "Our report concluded that the market would never deliver adequate security and the government must establish regulatory thresholds for critical infrastructure."¹¹ The overall market system dynamics, stakeholder perspectives, buying practices, technology, and vendor landscapes provide the evidence for this ongoing breakdown and help us understand how to solve it.

System dynamics and incentives

To understand the economics of the market it is helpful to describe the overall system. However, producing a fully comprehensive description of the cybersecurity market system would obscure the key dynamics. To that end, research interviews have highlighted the five key actors in the market and how they operate. The below graphic shows the actors, their context, overriding incentives and current efficacy, deliberately splitting out the Enterprise group into ‘Security buyers and users’ and ‘Leadership’ as their risk focus and understanding is often different.

EXHIBIT 6



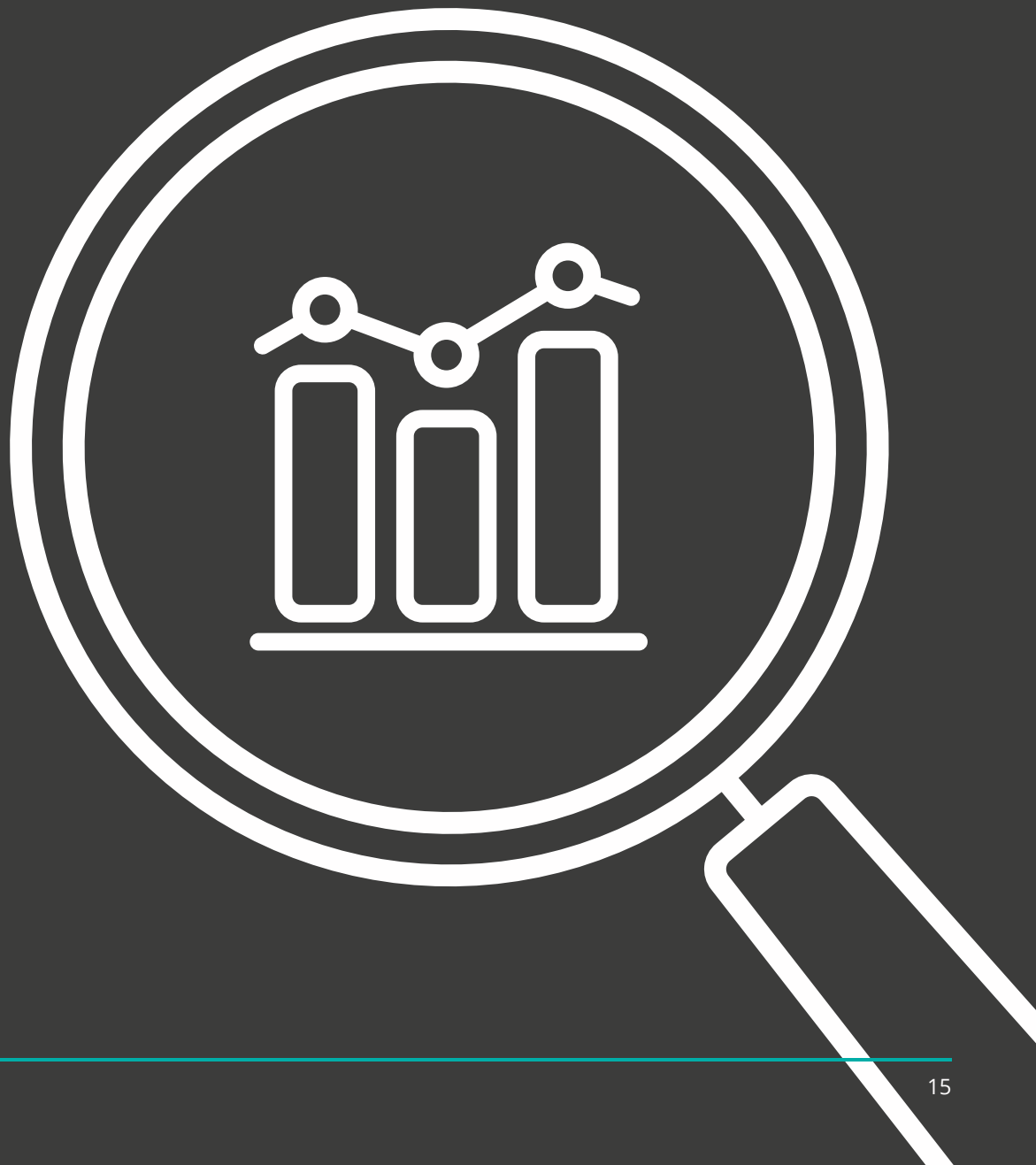
¹² SOURCE: Club CISO Report 2020

Clearly there are variations in the characteristics of each group depending on the enterprise, market sector or country, but this view captures the common structure. The key points to take away from this system representation are:

- The number of parties involved is high so any improvement that enterprise tries to drive has to take into consideration many dependencies and interactions.
- This is a system in great flux. Interviewees frequently refer to the high rates of change in technology, attacker skills and approaches, vendor landscape, enterprise strategy and regulatory stance. This flux is a key influencer on the behaviour of all the actors.
- Attackers don't have to operate within the same set of rules as the other parties in the system, skewing responses and hampering efforts to defend.

In the coming pages we will analyze the system dynamics and incentives, looking at each constituent part. The systemic view is important given the complexity involved. As the CISO of a globally leading bank put it, “we haven’t looked hard enough at the underlying problems...we need to drive change by looking at the total system.”

STAKEHOLDER VIEWS



Enterprise CISO/Buyer – 'the customer'

The modern CISO context is near-impossible given the challenges they face from many sides, as was highlighted in a ZDNet article from February 2020¹³ titled 'Average tenure of a CISO is just 26 months due to high stress and burnout.' Below we pick out 5 key challenges, but first it is illustrative to start with a quote from the CISO of a globally leading professional services company demonstrating these competing pressures and resultant issues:

"...in the confluence of accelerated technology adoption, business demands and evolving threats by actors who are not constrained by national laws and rules...sometimes for security solutions you need to take an approach of 'field it and then fix it'."

5 key challenges facing CISOs today:

- 1 Cybersecurity tooling: there are real challenges to get it to work.** Cybersecurity tools often require perfect execution to function effectively, with myriad controls and options available in set up. For example, even the configuration of standard firewalls can be challenging for cybersecurity experts, with one saying "establishing the correct operating settings and parameters for our company firewalls and knowing they were working effectively was extremely complex and even now I am not sure they are right, all this when we are still a small (<\$10m revenue) business. I just don't know how the bigger companies do it". This tooling issue is made even more difficult given legacy technology in the enterprise (both security and operational technology): understanding the interaction between all the legacy systems and the impact on efficacy is often near-impossible. CISOs highlighted that it is not uncommon to inherit legacy security technology and be unable to understand its functionality or impact, but that removing it is often not an option due to the fear of potential implications. These complexities in the maintenance and operation of technology are exacerbated by the difficulty of finding people with the skills to support it. The talent gap in cybersecurity can in part be linked to the challenges of using the technology. As one systems integrator put it "operational and implementation challenges given tooling difficulties create some of the greatest risk."
- 2 IT organizations: operations focus.** In the worst cases highlighted by interviewees the IT organization doesn't understand the security technology being proposed or used and cannot support implementation and maintenance effectively. Clearly, given they are in the same organization, the security and IT groups have aligned incentives and are 'on the same team', but often the broader operational pressures on the IT team are so great that security implementations or maintenance are compromised. This lack of capacity or capability to

prioritize security implementation is a very commonly cited issue by CISOs. For example, in a recent ClubCISO report, 37% of CISOs said they were uncomfortable with how well aligned security is with IT operations. This issue becomes all the more critical given that in most organizations almost all of the defensive technology employed is operated by the main IT organization.

3 Constant fire-fighting: reactive not proactive state. Given the pace of change and rate of attack CISOs are often being called upon to deal with short-term, high-impact, issues on a daily or weekly basis. The historical poor efficacy of protective security solutions means that the focus of defense in recent years has grown in the areas of monitoring, detection and response. While buyers have continued to spend on protection solutions, the fact that no protection can ever be perfect is often confused with an assumption that there is no point trying to do better, resulting in proportionally less effort from buyers to demand improvement. As observed by a senior cybersecurity advisor, “fire-fighting takes over the role given current issues – often CISOs don’t have the time to do a quality job.” This lack of time spent evaluating technology is highlighted by a recent ClubCISO survey that showed that the number 1 thing CISOs spent least time on was technology selection¹⁴.

4 Company Boards: demanding compliance. Boards face an evolving challenge as they have the legal responsibility to govern enterprise risk but are still getting to grips with cybersecurity risk management. Many are facing challenges defining their risk appetite given the nature of the threat they face (potentially existential, but often poorly defined). Without a clear view on risk appetite or threat then it is hard to govern the response required. This lack of clarity leads Boards to adopt a compliance-based approach to cybersecurity risk management. The compliance-based approach relies on meeting national or sector-based maturity standards during a third-party audit. Audits are gradually improving to focus on actual risk management performance rather than purely input characteristics related to processes and capabilities in place (eg. TIBER-EU scheme), however, much of the focus is still on inputs rather than a real test of cybersecurity resilience and risk reduction. As one banking CISO put it, “compliance assessments cloud the view; regulators will be satisfied if you buy the industry standard products.” The Board focus on compliance cascades through the Enterprise driving a focus on demonstration of process and capability rather than effective security. Giving Boards greater guidance on the demands they could or should be making of their organizations would help improve cybersecurity efficacy. As one financial services Chairman remarked, “Boards are open to improving, they just need to know which questions they should be asking to get assurance of compliance.”

¹⁴ <https://www.clubciso.org/downloads/>

5 Vendor relationships: challenged. A near universal issue for CISOs is their relationship with vendors, with almost none of them satisfied with the current situation. With 1000s of vendors on the market and new entrants coming every week CISOs have difficulty navigating the market. The breadth of claims made for products and the challenges in validating them mean many CISOs say they just stick with what they know and try to buy from well-known brands, independent of how well the technology is really working. The classic phrase 'you never get fired for buying IBM' was used multiple times to illustrate the drivers of customer decision making when buying. Given the rate of growth, vendors are incentivized to get to market quickly, but they also face a congested competitive landscape. To stand out in such a crowded market, vendors invest heavily in marketing and sales efforts, resulting in an overload of information and "white-noise" for buyers. FUD (fear, uncertainty and doubt) tactics and exaggerated claims about products and services are commonplace and when these claims can't be met it undermines the relationship between buyer and seller. "When vendors talk about selling 'military-grade' cybersecurity but then can't back up their claims, it hurts the market" said one engineering company CISO. This issue was highlighted in an article published by McKinsey titled 'Securing software as a service' from September 2019¹⁵, "More than 70 percent of respondents said that uninformed or misleading claims about security capabilities were a cause of dissatisfaction. Reportedly, some sales representatives even misrepresent certifications or customer references. One manufacturing company's CISO said, "I am sick of receiving glossy marketing materials, which are essentially snake oil when it comes to security features . . . many, many vendors will claim their security features are better than [what] a very simple assessment will reveal.'"

Enterprise Leadership

Enterprise leadership is primarily motivated to drive the performance, evolution and competitive positioning of their organization, while keeping within the bounds of regulation. Security is clearly important, and receives public support from leadership, but it is typically a hygiene factor that is assumed rather than thoroughly inspected. This stance is logical given the perceived risk and impact of attack; however, interviewees noted a marked difference (unsurprisingly) between leaders who had suffered a major, successful attack and those who hadn't.

After a successful attack, leadership engages more deeply with cybersecurity defense and assurance, asking deeper questions and prioritizing investments. Other company leaders will typically only benchmark their security efforts against peers (formally and informally) and adopt an approach of investing enough to keep up with the norm without 'over-investing' in time or money – on the basis that if they meet those norms, then even if a breach occurs they will have met their responsibilities.

Unless their organization has a specific strategic benefit from an enhanced security position then leadership do not feel incentivized to actively drive further improvement in security. In terms of their expectations of security the general view seems to include two components. First, it has become the conventional wisdom to assume that 'you will get hacked anyway, no matter what you do'. Second, it is assumed that differences in security technology efficacy in each category are insignificant. As one financial services Chairman explained, “Boards think you can't do much about cybersecurity efficacy, it is just down to ticking boxes and complying, make sure you are in the pack, you don't need to reinvent the wheel, don't need to be innovative.”

During our research, interviewees undermined these two major misconceptions: many respondents see efficacy issues and variations in security technology, implying that there is a spectrum of efficacy and that the more effort you make to have effective security, the less likely you are to get hacked. Clearly no security can ever be perfect – it is a truism to say that whatever you do, you might still get hacked – but if you have worked to have solutions that are at the more effective end of the spectrum then your risk profile will be better than your competitors, and you will suffer fewer successful attacks.

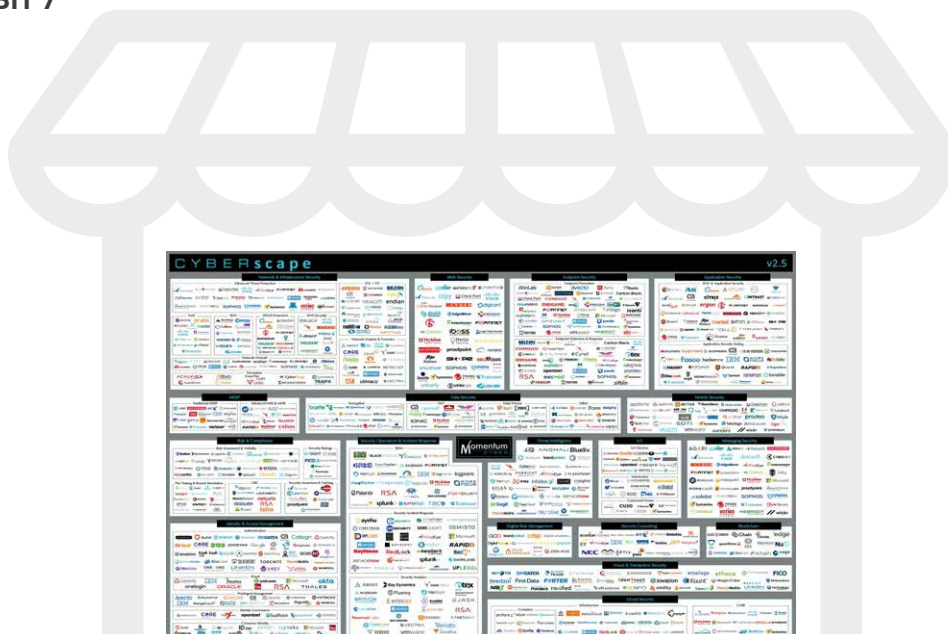
If leaders realize they are at real risk and that they can reduce the likelihood of successful attack by demanding more from their technology, then real improvement can be made.

Vendors and intermediaries

Vendors face an interesting paradox: a market that is growing rapidly every year but that is also already heavily crowded. The growth is attracting high rates of investment and driving aggressive business targets. The crowding means that vendors need to be highly visible and active in their marketing efforts to get customers' attention.

The below 'Cyberscape'¹⁶ is a well recognized representation of the busy market and the quotes are illustrative of the issues it causes.

EXHIBIT 7



Many interviewees recognise the cybersecurity market is congested

"We have to rely on partners to help us navigate the vendor market because it is so busy, it's very difficult to keep up"

Consulting CISO

Some believe the congested market is an indicator of failure

"We wouldn't have as many solutions in the market if they were all doing a great job"

International Logistics CISO

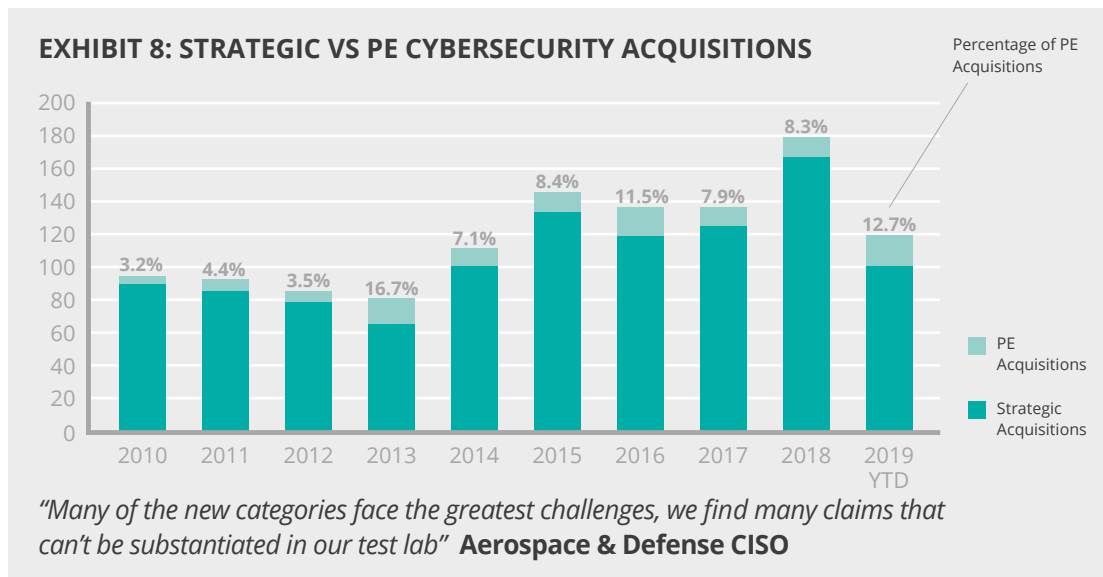
Congestion can stifle innovation

"It's very hard for new vendors to break in... unless you are the 'hot new thing' then you don't get any air-time"

Supply Chain Risk Assessor

Given the pressure to grow and to fight for market share in this already congested space, vendors are incentivized to bring products to market even with only minimum viability. This issue led one CISO to observe “typically when we see newer technology it is only 60-70% complete and we end up having to effectively do the final development for the vendor in order to make the solution work properly.” In the worst cases, anything that hampers speed to market will be put under pressure and questioned, even if this is in the areas of technology functionality or operation. The notion of what constitutes a Minimum Viable Product in cybersecurity is potentially something to be debated.

The high investment rate and volatility in the vendor space is also common knowledge with volumes running at strong levels, and growing, over the last decade.



The rate of change creates an interesting second order effect that interviewees commented on. Apparently, when companies go through an IPO or significant ownership change then key talent often leaves in search of the next challenge. This loss of talent then has an impact on the continued development and improvement of the technology, shortening its useful shelf-life. As the founder of a globally leading technology assessment company said (based on their years of assessing technology efficacy), “after key employees can monetize their shares the efficacy of the solution starts to drop, every company that is a ‘rocket-ship’ suffers because of this, the talent starts to leave after you can sell your shares.”

SOURCE: Hampton
M&A market report 2H
2019 Cybersecurity

The previously mentioned high levels of marketing efforts in cybersecurity have also been studied before. Peter Cohen¹⁷ described an industry ‘addicted to marketing’ and CISOs we have interviewed also remarked on the issue.

EXHIBIT 9

“The world’s largest cyber security firms spent startling amounts on sales and marketing last year, allocating 41% of revenue to their commercial activities. Indeed, some companies exceeded 50% and even 60%. When compared against other B2B tech firms such as Cisco, (19%) or Microsoft (17%), it’s clear that the cyber security industry is somewhat different in the way it carries out its business.”

Peter Cohen, Feb 2018

“The market is too busy to navigate, all the vendors spend so much money on marketing and events that you end up not really being able to differentiate, the major conferences highlight this problem”

Electronics CISO

A BRUTAL INVESTMENT IN PERSUASION¹⁷

These are the top six cyber-security focused firms who submit publicly available annual reports. We can see they have combined revenue of \$9.8 billion, with a sales and marketing expenditure of \$4.1 billion.

	Revenue (\$millions)	Sales & Marketing Spend (\$millions)	Sales & Marketing Spend (\$millions)
Symantec	4,019	1,459	36%
Palo Alto	1,761	919	52%
Fortinet	1,275	626	49%
FireEye	714	439	62%
Checkpoint	1,741	420	24%
Proofpoint	375	201	54%
Cyber Average	1,648	677	41%

Top six cyber security firms by revenue FY 2016/17

Given \$90 billion or so spent globally on cyber security in 2017 we can estimate that somewhere around \$25-\$35 billion mark was spent last year convincing you to buy more cyber. That’s up to \$110 million *per day* in sales and marketing.

What is it about cyber security industry that necessitates such a brutal investment in persuasion?

The above issues notwithstanding, vendor leadership typically remains committed to delivering high-quality solutions and generally ‘believe in the mission’. However, a couple of CISOs remarked on observing issues creeping into the lower layers of vendor organizations in the form of short-cuts in product coding or making excessive capability claims. This is an understandable challenge for vendors who are working hard to bring new solutions to the market and are under pressure to move quickly. The internal cascade of this pressure can result in sub-optimal decisions that are not then visible to the leaders of the organization (the old adage that it is hard to speak truth to power seems to fit here).

Intermediaries are also a key component in the market and aim to play a role in supporting improvement. Three groups were highlighted during the interviews and their situations described.

EXHIBIT 10



SYSTEMS INTEGRATORS AND RESELLERS

Ideal function:

Advisors to end customers on best technologies and practices. Support with technology selection, operations and innovation.

Current approach:

Typically incentivized to be conservative and risk averse with technology selection. Technology typically included in the portfolio only when it is an industry standard. Even though the larger businesses have strong testing capability the incentive to use a 'tried & trusted' solution is still greater.

Issues:

The benefit of assessing for efficacy doesn't outweigh the current cost as they can select industry standard solutions and still deliver on customer expectations.



ASSESSMENT & TESTING ORGANIZATIONS

Ideal function:

Provide independent, detailed, assessment of solution efficacy covering all the elements (capability, practicality, quality and provenance).

Current approach:

Typically focus on assessing functionality against vendor claims without doing deep assessment of efficacy as budgets are limited. Vendor capabilities mostly assessed based on questionnaires rather than actual physical audit. However, there are selected labs that do provide deep assurance services of a high quality.

Issues:

Cost is an issue for customers with limited budgets, many of them are happy to trust the free advice from their peers rather than pay for their own test.

Vendor relations are also fraught given the obvious conflicting incentives and can end in dispute (e.g., CrowdStrike vs NSS Labs in 2017)



INSURANCE

Ideal function:

Provide an incentive for buyers to invest in effective security to reduce risk and premiums. Provide guidance on risk reduction approaches and methods. Provide insurance backed warranties for solution vendors.

Current approach:

Insurers are struggling to gain traction with buyers and vendors. Insurance is often sold based on cybersecurity risk assessors input (they have guided 41% of insurance policy purchases in the US). Warranties are being issued based on marketing collateral.

Issues:

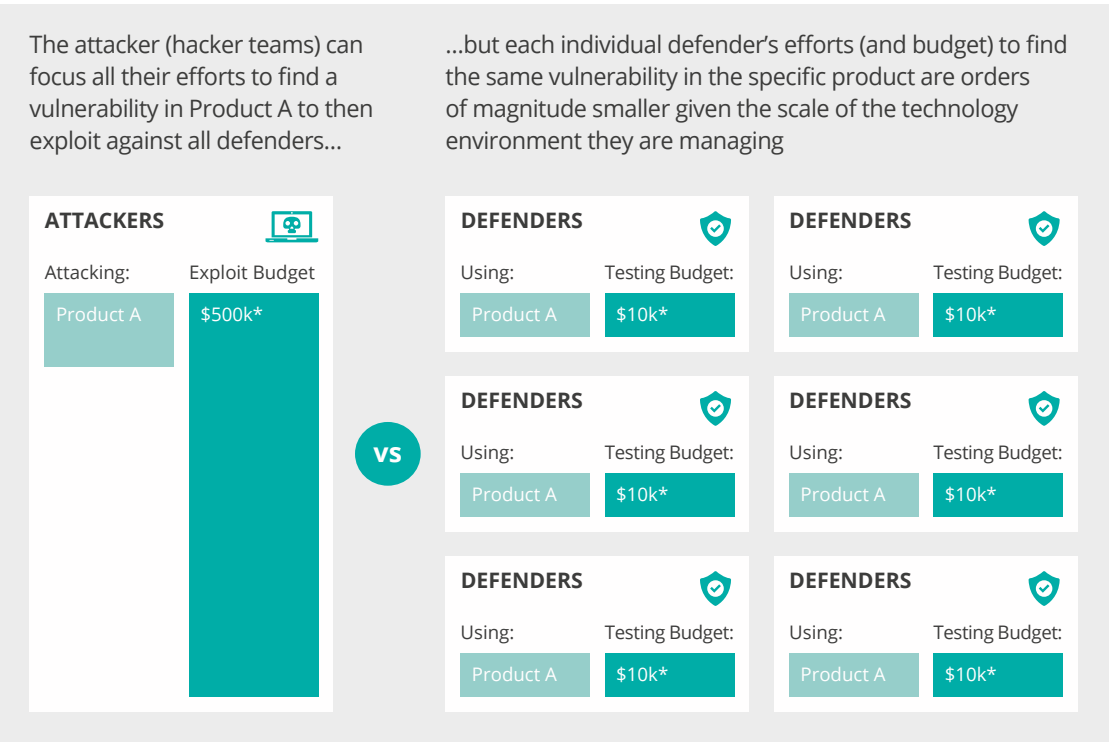
There is a perspective that many policies are being written without detailed risk or capability assessment, this is possible because the actual coverage is weak and claims are heavily capped.

Insurance backed solution warranties are devalued because they are too easy to get, while in reality accepting marketing collateral at face value is not effective.

Attacker

Interviewees confirmed the view that there is an imbalance between attackers and defenders in terms of concentration of effort. Attacker economics are such that they can afford to invest deeply to find vulnerabilities in single technologies which they can then leverage across multiple organizations (as was seen with the ransomware wave of 2019¹⁸). However, defenders don't have the resources to perform equivalently deep vulnerability assessment on every solution they employ. To do so would be prohibitively expensive, especially as part of a procurement funnel process where more solutions would need to be assessed than purchased. Only around 20% of CISOs in the cohort proactively mentioned using penetration testing and only a couple were spending significant amounts (eg. >\$10k per test).

EXHIBIT 11



*Representative numbers

¹⁸ <https://www.cbronline.com/news/ransomware-2019>

Regulator

Many interviewees see the regulatory and standards landscape as complex and immature in cybersecurity, with only 35% of CISOs proactively mentioning certification or standards as part of their technology selection process. Standards are set for both customers and vendors. There are also both compulsory and voluntary schemes depending on sector and country of operation. Standards are typically set by a sector or national body and then assessed by independent audit organizations.

User standards take several forms

EXHIBIT 12

User standard examples

Government secure organizations internal standards

Government open organizations internal standards: UK MCSS, US FISMA (Federal Information Security Management Act), IAF/CSF, ISACA

Maturity frameworks: US NIST, UK CQUEST

Vulnerability and intelligence sharing & testing: UK CBEST/CISP, TIBER-EU, ISACs

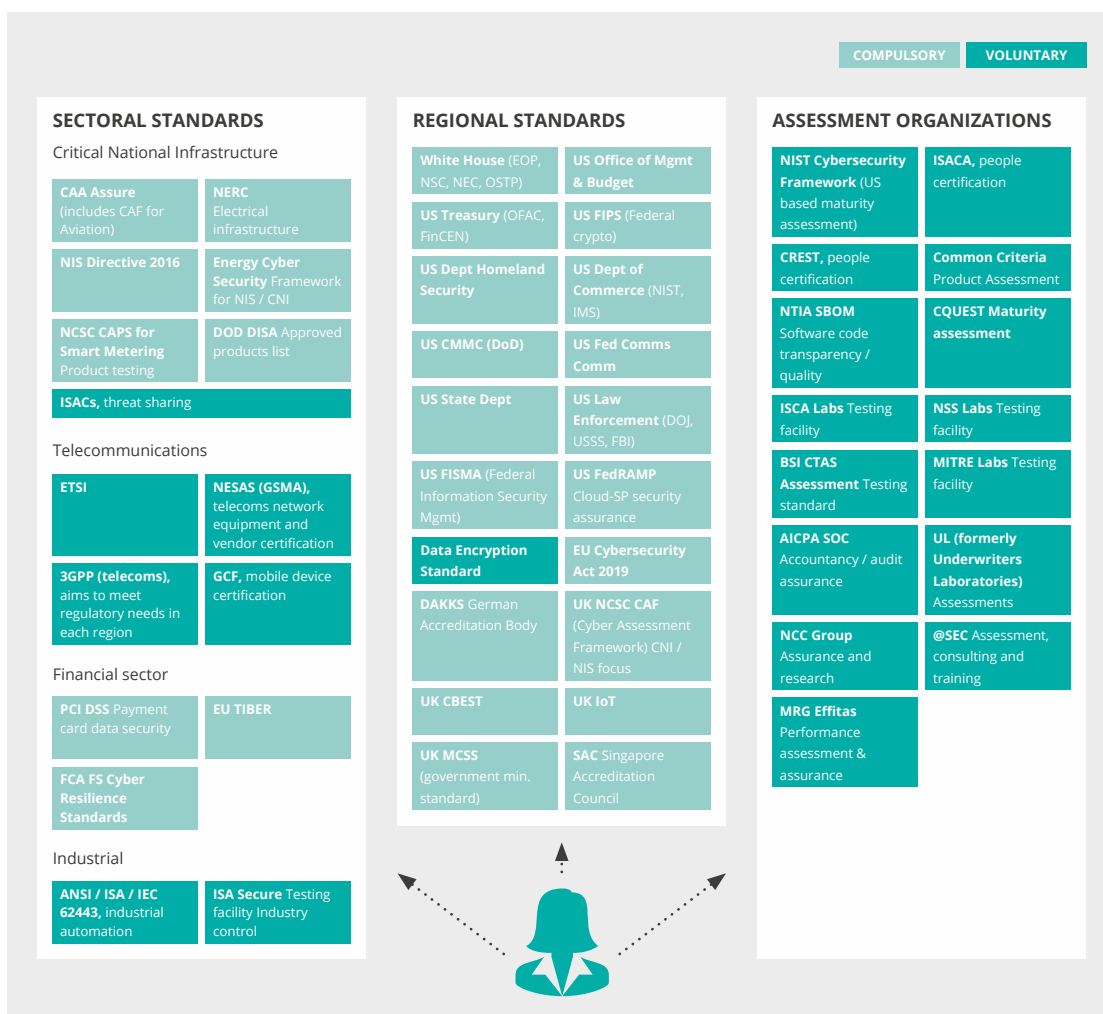
General management standards: ISO 27001

Sector specific standards: CPMI-IOSCO, NERC (North America Electric Reliability Corporation) CNI/industrial focus, ANSI / ISA / IEC 62443 (part of ISO 17065, focus on industrial automation) & ISCI (includes product certification), ETSI (ICT)

National accreditations: Germany (DAkkS, BSI), Singapore Accreditation Council

Vendors face a more complex landscape of compulsory and voluntary regulation and standards, which makes it hard for buyers to assess and demand the right assessments or certifications. This is notwithstanding all the hard work and engagement of vendors over many years to support development of ISO and other standards, it should be recognized that vendors have contributed strongly and positively to the development of the sector.

EXHIBIT 13



The four key issues that arose in interviews around current regulation were:

1 Understanding: standards aren’t widely understood or known by buyers and users.

The complex nature of standards (eg. Common Criteria) makes it difficult for users - and in particular the leadership of customer companies - to evaluate them or to know which to use and demand when buying technology. Even vendors face challenges identifying what they need (or even have), as one remarked, “I don’t know what standards and certificates we have, let me look and get back to you...”

2 Efficacy: standards aren’t always effective measures of security. Many user standards focus on business process and behavior rather than on technical system efficacy. Many vendor standards focus on method and implementation quality rather than the inherent security of the solution. A banking CISO remarked, “if we ask for anything it would be the standard ISO type stuff”, which doesn’t provide any assurance on the actual efficacy of the solutions delivered.

3 Demand: standards aren’t widely and consistently demanded by buyers in the market. Buyers rarely refer to security efficacy standards when buying products, typically focusing on the solution’s functionality and ability to integrate rather than the core security efficacy. Vendors on the other hand do acquire and cite standards, but typically only when driven to do so by highly sophisticated customers. One CISO remarked that, “Quality is assumed. If they are selling to enterprises and have a good reputation, or an analyst or peer recommends them, then we assume the quality is OK.” While a vendor remarked that, “Procurement teams promote other factors meaning that efficacy is pushed further towards the bottom of the list of priorities.”

4 Innovation: some fear of regulation and standards stifling innovation, but it isn’t over-riding. When prompted, there was strong concern that any new standards would stifle innovation as they could not possibly keep up with the rate of new solution development, however, interestingly, fewer than 10% of CISOs brought this up proactively. The point was made that not only is it difficult to write standards on technology that can encompass future development, but also that the regulatory bodies and standards setters are typically not staffed by people with deep technical expertise, so find it hard to effectively regulate. Notwithstanding the concerns, 40% of CISOs and 25% of vendors proactively mentioned the need for regulation. Additionally, it should be noted that when regulation was discussed, EU-GDPR typically came up as an example of a big regulatory change. It was mostly brought up in the context of ‘evidence that regulatory change can happen, be effective and successfully raise awareness’. As one high profile expert put it, “one of the real benefits of GDPR is that it has forced us to do some house-keeping on our data that we hadn’t bothered to do for 20+ years”.

On the topic of EU regulation, it is worth noting that the Cybersecurity Act 2019 was recently passed, with two main objectives:

- **Revamp and strengthen the EU Agency for cybersecurity (ENISA)**
- **Establish an EU-wide cybersecurity certification framework for digital products, services and processes**

The certification component gives ENISA a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes and informing the public on the certification schemes as well as the issued certificates through a dedicated website. The certification schemes have some elements for consideration:

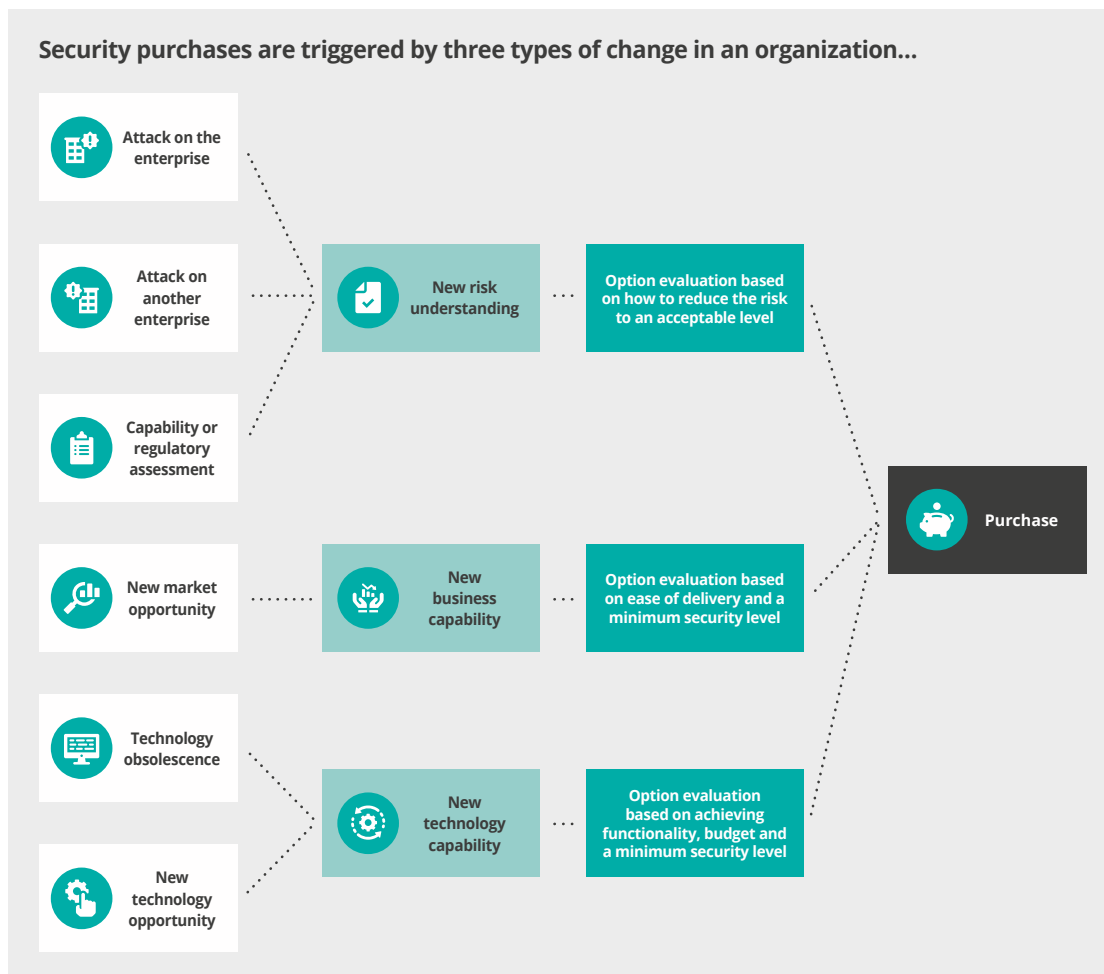
- **Common:** companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognized across the European Union.
- **Category schemes:** multiple schemes will be created for different categories of ICT products, processes and services.
- **Specification:** each scheme will specify type or categories of ICT products, services and processes covered, the purpose, the security standards that shall be met (basic, standard, high) and the evaluation methods (self, 3rd party). The schemes will also indicate the period of validity for the certificates issued.
- **Definition:** ENISA, upon request from the Commission or the European Cybersecurity Certification Group (composed by Member States), will prepare the certification schemes that will then be adopted by the Commission through implementing acts.
- **Validation:** alongside third-party certification, conformity self-attestation by the manufacturer is allowed for the products that present low levels of risk.
- **Voluntary / mandatory:** while the certification will remain voluntary, the Commission will assess whether mandatory certification is required for certain categories of products and services.

If this approach to certification can simplify and standardize approaches to cybersecurity then it could benefit users, buyers and vendors. Given the fragmentation in approaches around the world today, alignment and leadership are welcomed, so long as the standards are effective.

Buying processes

Given the context of each of the stakeholders involved, buying processes have evolved to serve the market. Security purchases are triggered by three types of change in an organization: new risk understanding, new business capability or new technology capability. The details of these triggers are shown below:

EXHIBIT 14



During the interviews two archetypal scenarios were identified when the efficacy prioritization of the technology to be purchased would vary according to need:

1 'High' efficacy focus: security buying based on reducing risk to an acceptable (typically lower) level.

Primary factors for consideration are:

- a. Evidence of efficacy and resilience
- b. Ease of integration and use
- c. Peer input
- d. Future-proofing
- e. Budget

2 'Low' efficacy focus: security buying based on meeting a market norm.

Primary factors for consideration are:

- a. Basic technical and operational fit
- b. Conforms with market norms
- c. Budget
- d. Ease of integration
- e. Enabling agile development
- f. Supporting cloud-based operating models
- g. Delivering productivity gains

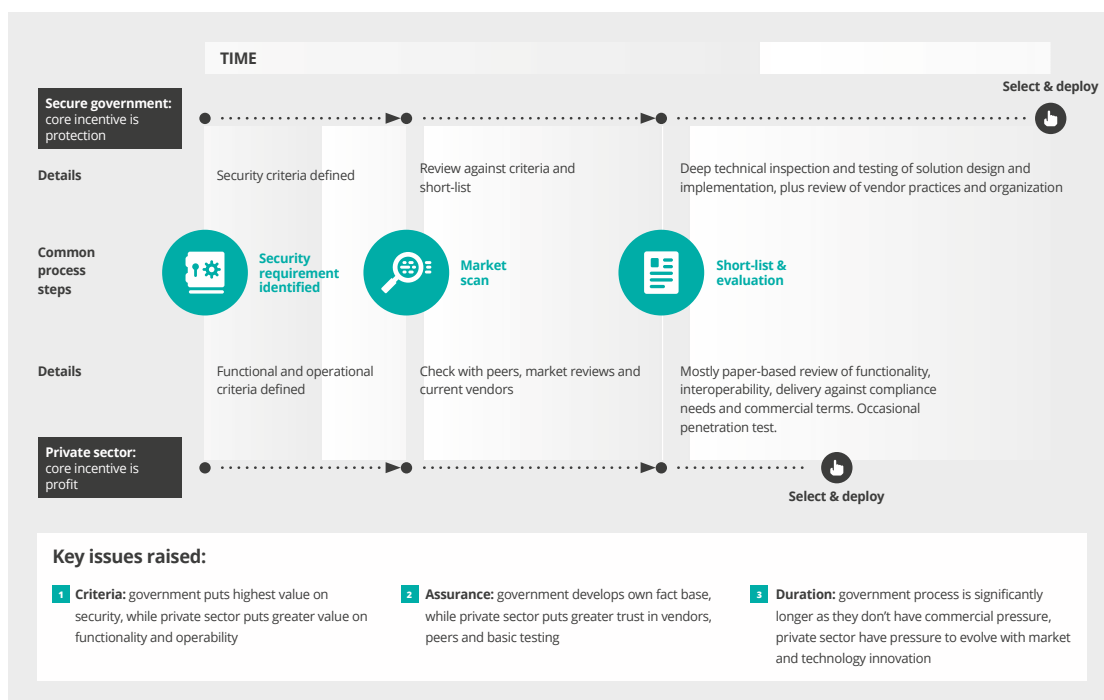
Note that 'Ease of integration' and 'Budget' are common factors to both environments. These were highlighted in many interviews as core factors for consideration when purchasing security technology. It's also worth noting that the above scenarios are often complicated by the 'portfolio view' when investments in different categories of security impact each other.

The actual buying process in almost all organizations follows a similar flow, with the major variation being in the depth of due diligence undertaken by the buyer. This variation is most starkly observed when we compare buying behaviour in the private sector and in secure government. It is understood that the private sector does not necessarily need to meet the level of security achieved by the most sophisticated government agencies, but the example is useful to highlight the discrepancy.

CYBERSECURITY TECHNOLOGY EFFICACY IS CYBERSECURITY THE NEW “MARKET FOR LEMONS”?

While the short-term approach to buying follows similar steps, the details of how the steps are executed are very different in each track:

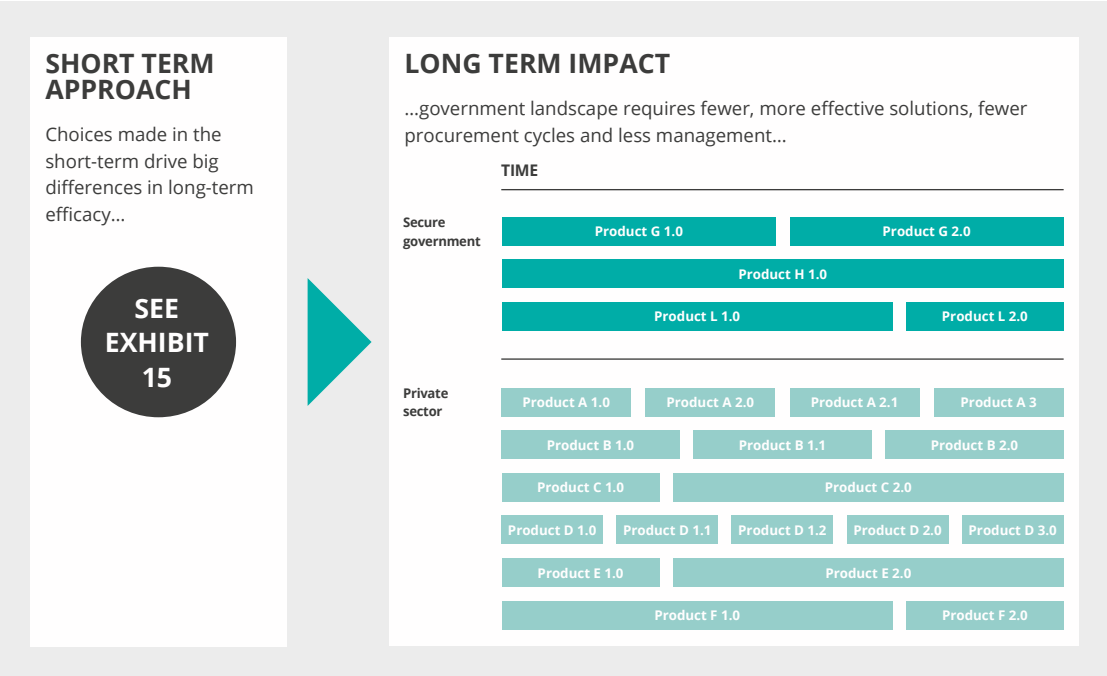
EXHIBIT 15



At the most sophisticated levels the private sector does start to emulate secure government, but this is only seen in a handful of global organizations. As one CTO and security expert put it, “I estimate that 80% of organizations don't really investigate whether the tool does its job, they are just trying to meet a compliance objective. 19% of organizations will interrogate the new tool and check logs etc., while only 1% will actually perform a full gamut of tests and assessments to assure the efficacy of the solution.” When this quote was tested with some other interviewees the estimates were broadly supported. It is worth noting that more than 50% of CISOs proactively referred to peer input as a key part of their buying decision, if so, are they all depending on the well-qualified input of the ‘1%’, or should they be more skeptical about peer input?

This variation in approaches to technology selection has a knock-on effect on the technology landscape observed in each environment. In the long-term, the secure government technology landscape is simpler and more effective (and potentially reducing cost overall) but more operationally rigid, as is shown in the exhibit below.

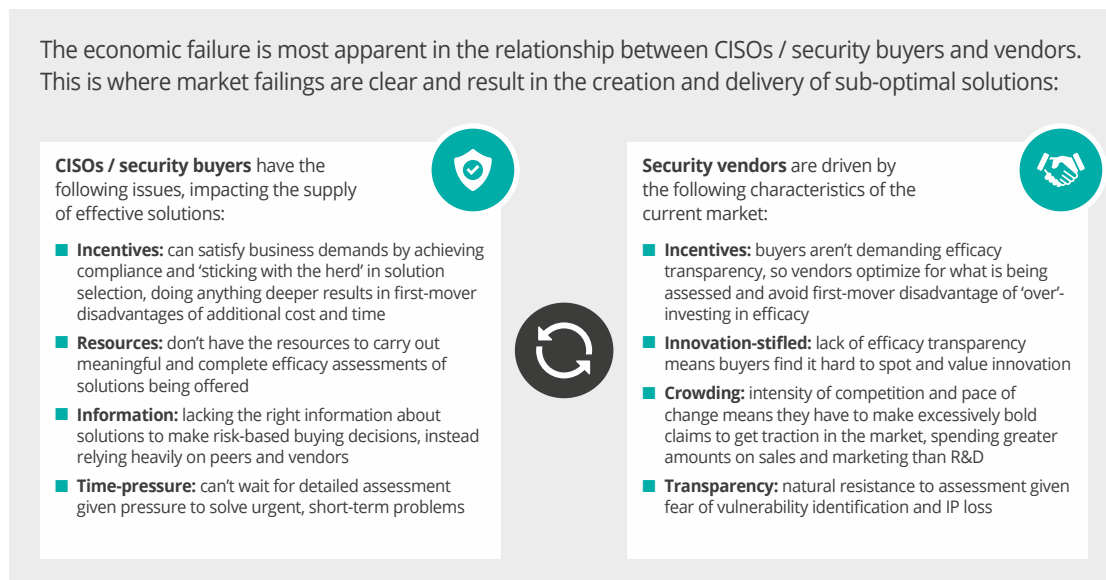
EXHIBIT 16



The resultant market breakdown

Having understood the system overview, the stakeholders’ perspectives, and the resultant buying process, the core breakdown in the market can be crystallized in the relationship between the buyer and seller. The relationship between CISOs / security buyers and vendors is where the market failings are most clear and result in the creation and delivery of sub-optimal solutions. Both parties find this relationship difficult. The exhibit below summarizes the issues:

EXHIBIT 17



“CISOs need better transparency on product limitations when buying, wouldn’t necessarily stop the sale, but would help to more effectively deploy and operate solutions...”
Global Bank CISO

Broken markets have been studied in the past and the lessons learnt on how to fix them. Akerlof’s 1970 paper¹⁹ identified the market for “lemons” which highlights some of the basic characteristics of failing markets. Some key characteristics of a ‘market for lemons’ are:

- Information asymmetry between buyer and vendors (potentially varied according to buyer aptitude), can work in both directions
- Existence of goods discovered to be defective after purchase (aka “lemons”)
- Lack of incentive to develop and sell “peaches” (aka high quality)
- High quality ‘driven from market’ by existence of lower cost “lemons”
- Lack of credible, common, quality assessment available to buyers

¹⁹ <https://viterbi-web.usc.edu/~shaddin/cs590fa13/papers/AkerlofMarketforLemons.pdf>



Akerlof's Market for "Lemons": Quality, Uncertainty and the Market Mechanism - George A. Akerlof (1970) Quarterly Journal of Economics

Akerlof won the 2001 Nobel Memorial Prize in Economic Sciences for this and other research into information asymmetry.

"Many customers don't have the capability or capacity to assess cybersecurity solutions properly before buying..."

Cybersecurity Vendor

His 1970 paper describes the market problem in detail:

- **Information asymmetry:** Akerlof's research examines how the quality of goods traded in a market can degrade in the presence of information asymmetry between buyers and sellers, leaving only "lemons" behind
- **Detailed market dynamics:**
 1. Suppose buyers cannot distinguish between a high-quality product (a "peach") and a "lemon"
 2. Then they are only willing to pay a fixed price for a product that averages the value of a "peach" and "lemon" together (p_{avg})
 3. But only sellers know whether they hold a peach or a lemon
 4. Given the fixed price at which buyers will buy, sellers will sell only when they hold "lemons" (since $p_{lemon} < p_{avg}$) and they will leave the market when they hold "peaches" (since $p_{peach} > p_{avg}$)
 5. Eventually, as enough sellers of "peaches" leave the market, the average willingness-to-pay of buyers will decrease (since the average quality of products on the market decreased), leading to even more sellers of high-quality products leaving the market through a positive feedback loop
- **The result is that high-quality is driven from market:** the uninformed buyer's price creates an adverse selection problem that drives high-quality products from the market
- **Leading to market failure:** adverse selection is a market mechanism that can lead to a market failure.

CYBERSECURITY TECHNOLOGY EFFICACY IS CYBERSECURITY THE NEW “MARKET FOR LEMONS”?

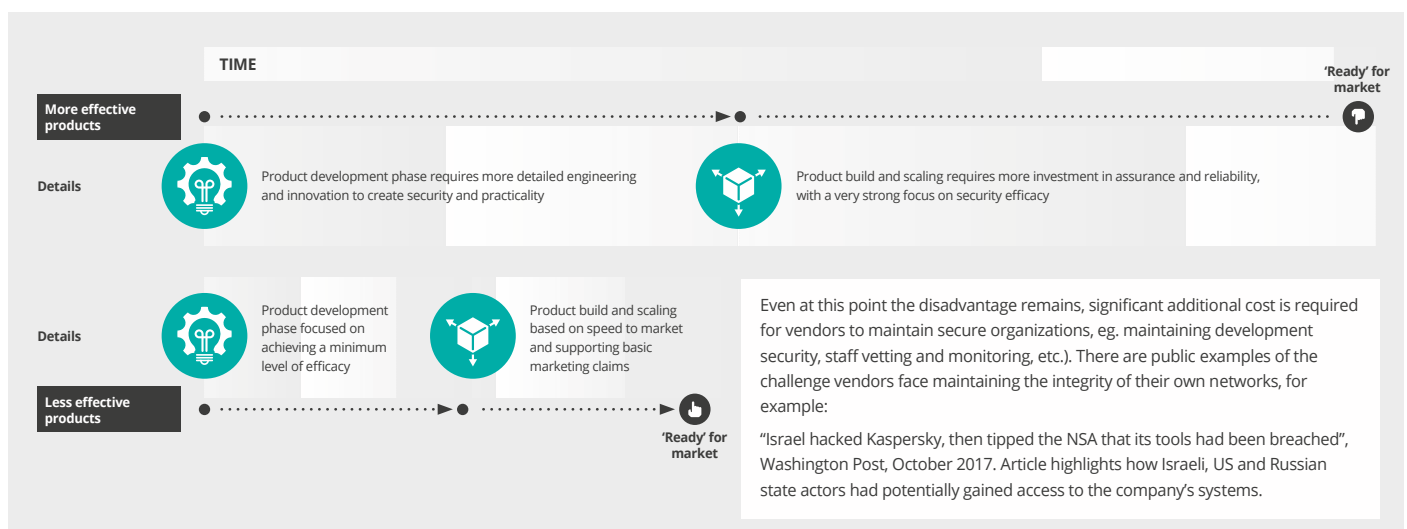
This leads to the following conclusions:

- **No incentive for peaches:** with information asymmetry the market tends towards being dominated by lemons as they are the only economic products to sell
- **Vendor perspective:** as quality is indistinguishable beforehand to the buyer (due to the asymmetry of information), incentives exist for the seller to pass off low-quality goods as higher-quality ones
- **Buyer perspective:** takes the vendor incentive into consideration and assumes the quality of the goods to be uncertain. Only the average quality of the goods will be considered, which in turn will have the side effect that goods that are above average in terms of quality will be driven out of the market
- **How does it work in reality?** Not all players in each market have the same aptitude to assess quality, resulting in a distinct advantage for some vendors to offer low-quality goods to the less-informed segment of a market that, on the whole, appears to be of reasonable quality and have reasonable guarantees of certainty. This is part of the basis for the idiom “buyer beware”.

To solve this problem in the cybersecurity technology market would require first-mover disadvantages for both parties to be overcome.

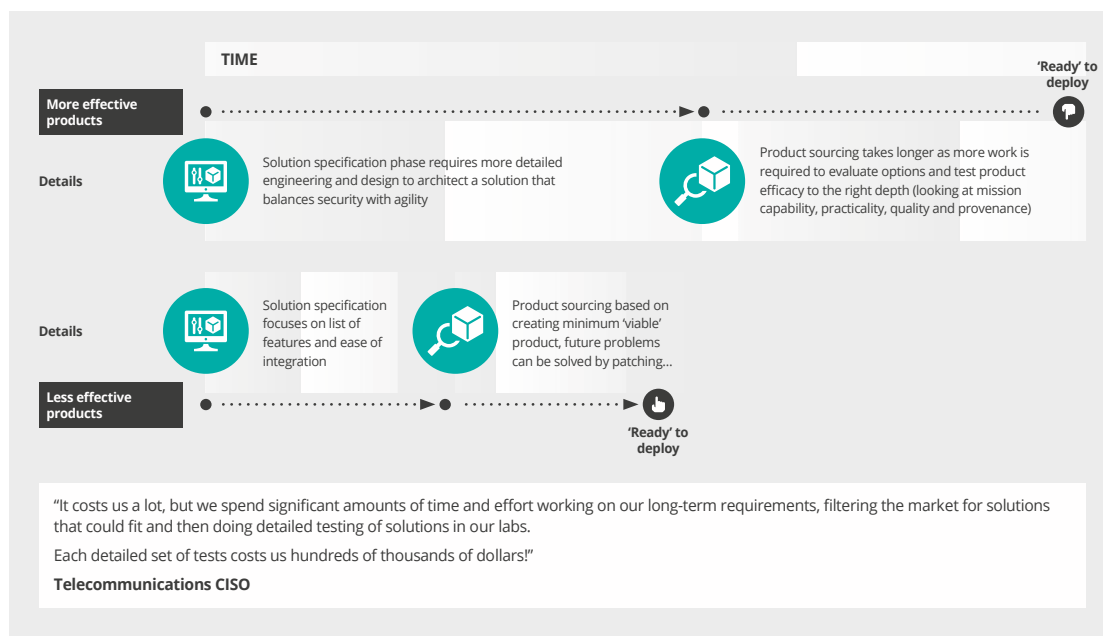
The first vendors of cybersecurity that create more effective products take on a burden that makes them uncompetitive, as is shown below in this explanation of their first-mover disadvantage:

EXHIBIT 18



In the meantime, the first buyers of cybersecurity that demand more effective products take on a burden that makes them uncompetitive as it costs them more to procure solutions and they take longer to deploy. Their first-mover disadvantage is described below:

EXHIBIT 19



Overcoming these first-mover disadvantages and the incentives of each market player will be necessary in order to kick-start change and drive greater efficacy in cybersecurity technology.



3

INDEPENDENT TRANSPARENT TECHNOLOGY ASSESSMENT IS THE SOLUTION

Solving the economic problem requires a new model, creating new incentives for vendors and new approaches for buyers. Around 2/3 of research participants believe independent efficacy assessment of technology is required to solve the information asymmetry.

Independent (and transparent) efficacy assessment would enable buyers to make risk-based purchasing decisions by providing them with better information and would give vendors stronger incentives to deliver technology with improved efficacy. Over time, improved technology would reduce the likelihood of successful attacks and would have the additional benefit of reducing dependency on people and process. Improved efficacy transparency would also help organizations govern risk more effectively and differentiate security investments towards priority areas. From a vendor perspective, efficacy transparency would help new innovations penetrate the market, reducing the need to spend excessively on marketing and sales to gain traction.

Clearly detailed efficacy assessment isn't without risks and issues. First, assessments need to keep up with and support technology innovation. To that end it would be sensible for market standards to be set for assessments, rather than technologies (as discussed previously). Assessment standards already exist in other markets and in niches of security today (eg, GSMA NESAS²⁰): they allow technology innovation to continue, as the standard focuses on the key principles of assessment rather than on technical details. Second, the cost of efficacy assessment shouldn't be under-estimated. This is a key reason behind the lack of current assessment as individual enterprises typically can't afford to do it properly. Whatever solution the market selects will need to find a way of fairly distributing the cost so that, shared across the buying community, the costs become affordable.

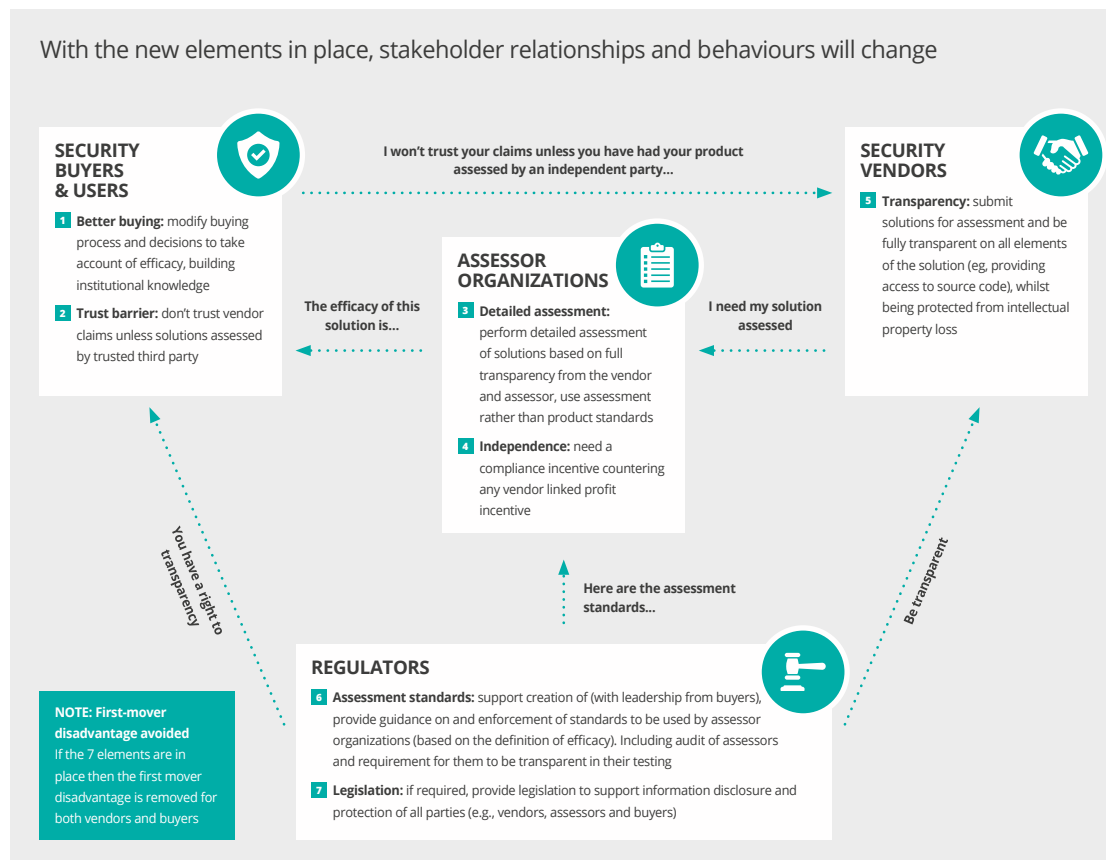
²⁰ <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>

The new model

The aim of this research is not to define a single new model but rather to highlight an issue and start an industry debate. However, during the interviews and related discussions a rough consensus around a new model has started to emerge.

The proposed model includes seven elements for solving the market for lemons, each with a specific owner. As above, we expect this model to evolve as public debate on the topic progresses; this is not a definitive solution but more a proposal. The exhibit below shows the seven elements and their owners:

EXHIBIT 20



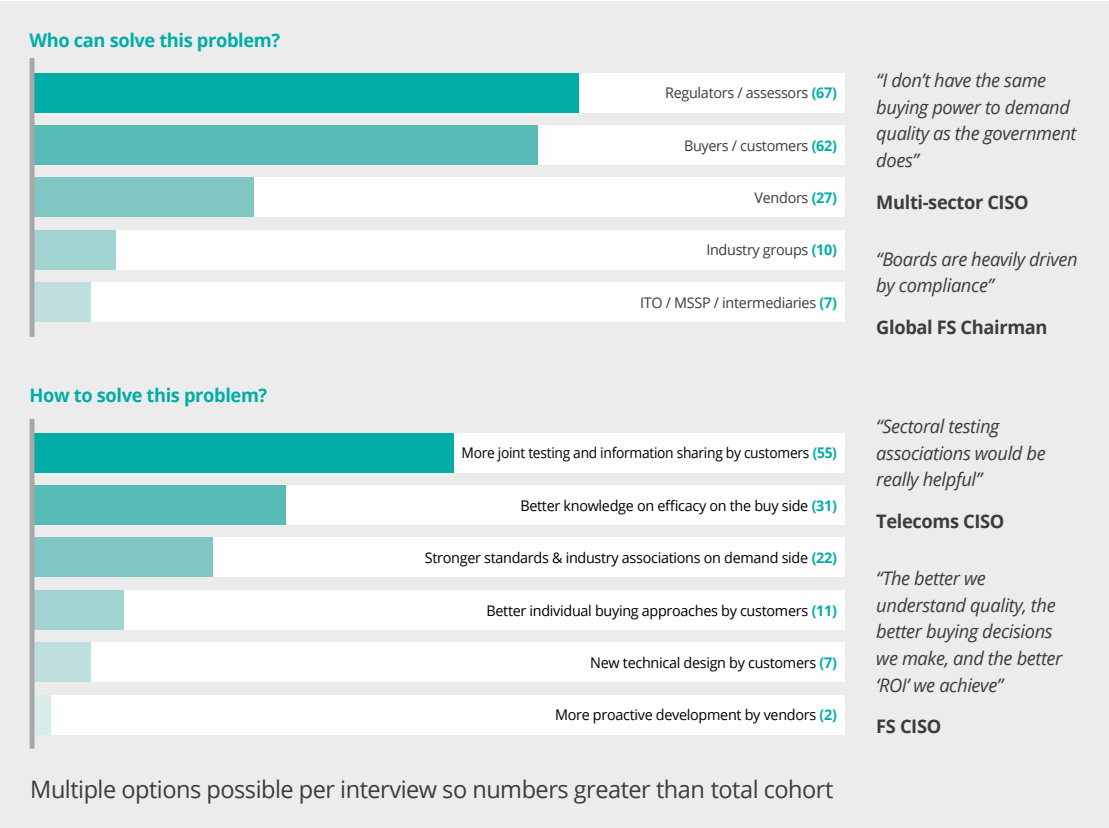
There is a rationale for each element of the new model, as described in the exhibit below:

EXHIBIT 21

Lead Stakeholder	Elements	Rationale
Security buyers & users 	<ol style="list-style-type: none"> Better buying: modify buying process and decisions to take account of efficacy, building institutional knowledge Trust barrier: don't trust vendor claims unless solutions assessed by trusted third party 	<ul style="list-style-type: none"> Buying decisions that take into account solution efficacy help organizations materially reduce risk and incentivize vendors to develop and sell more effective products, the increased knowledge removes the information asymmetry from the market The lack of trust is required in order to give the vendors an incentive to get their products assessed
Assessors 	<ol style="list-style-type: none"> Detailed assessment: perform detailed assessment of solutions based on full transparency from the vendor and the assessor, use assessment rather than product standards Independence: in order to remain independent they need a compliance incentive countering any vendor linked profit incentive 	<ul style="list-style-type: none"> Detailed assessment is required to redress the information asymmetry, and the assessment standards are required to make assessments comparable (product standards won't work as they slow innovation), assessments must be transparent to be trusted The compliance incentive is required to counter the potential profit incentive of attracting more vendors by lowering assessment rigour
Security vendors 	<ol style="list-style-type: none"> Transparency: submit solutions for assessment and be fully transparent on all elements of the solution (eg. providing access to source code), whilst being protected from intellectual property loss 	<ul style="list-style-type: none"> Vendors are required to submit their solutions in order that an independent organization can execute the assessment, full transparency is required in order for the assessment to work and protection from intellectual property loss is required as assessors will see confidential details of the solutions
Regulators 	<ol style="list-style-type: none"> Assessment standards: support creation of (with leadership from buyers), provide guidance on and enforcement of standards to be used by assessor organizations (based on the definition of efficacy). Including audit of assessors and requirement for them to be transparent in their testing Legislation: if required, provide legislation to support information disclosure and protection of all parties (e.g., vendors, assessors and buyers) 	<ul style="list-style-type: none"> Common standards for assessors are required to enable multiple organizations to operate as assessors and for vendors to understand what standards the assessors will work to (for example, ISO/IEC 17065 is the common standard for certification bodies) Protective legislation is required for each stakeholder to give confidence in the system and to reduce the risk of dispute

This model was derived during the 100+ interviews conducted, with testing and review of the conclusions during highly engaging follow up calls and document reviews by the cohort. In terms of the original inputs from the interviewees (before the idea of the new model was shared – thus avoiding bias) the exhibit below shows the frequency of mentions for who should solve the problem and how it should be solved. The frequencies add up to more than the number of interviewees given they could mention more than one party to solve the problem and more than one method to solve it. The quotes are also illustrative of the views of the cohort.

EXHIBIT 22



The benefits of the new model

There was broad enthusiasm among the interviewee group for the benefits a new model could bring. CISOs felt that it could make technology selection easier and more efficient, while vendors felt that it could ‘level the playing field’ and allow innovation to break through more easily. All participants agreed that standards set on assessment rather than technology were a more sustainable and effective way of driving improvement considering the low confidence that technology standards can keep up with the rate of innovation.

5 main benefits of the new model were highlighted during the interviews and follow up discussions:

- 1 More effective cybersecurity solutions:** by demanding transparency on efficacy before a solution is brought to market, the vendor is incentivized to invest more in efficacy. Users expect improvements in capability to match claims, more practicality (especially around integration and operation) and fewer vulnerabilities linked to quality problems.
- 2 Better transparency on security efficacy:** with a common view on the efficacy of technology before acquisition, it is easier to evaluate the efficacy of technology in operation, supporting enterprises to identify vulnerabilities and increase resilience.
- 3 Better ability to set risk appetite:** with greater clarity on the strength of technical defenses, enterprises can better define their risk appetite, as it can be defined in terms of the efficacy of the solutions required to protect the asset in question.
- 4 Better differentiation of security towards priority areas:** the concept of ‘protecting the crown jewels’ is not new to cybersecurity (or any other form of security). However, with greater clarity on the efficacy of security technologies, enterprises can select the most effective solutions (typically more expensive and onerous operationally) to protect the most important assets.
- 5 Better correlation between spend and efficacy:** given the ability to evaluate security technology efficacy, the enterprise will be able to make better informed value trade-offs between solutions, allowing them to spend money on validated efficacy rather than hope. While greater transparency on efficacy won’t provide for an absolute ‘return-on-investment’ calculation it will help organizations trade-off options for solving their organization-specific risks.. In this model, customers are obviously allowed, and better able, to make their own risk-based decisions. If they want to buy less effective products for other (non-security) reasons then they should do that – but they will do so in the full knowledge that this is what they’re doing.

Open issues

Clearly massive changes in the way an industry operates are not simple or easily achieved and the interviews have highlighted and confirmed some of the open issues. The two issues that came up most frequently were around payment (as mentioned previously) and assessment dispute.

In terms of payment and the high costs of assessment, the structure for the new approach remains to be confirmed. We have heard and debated four options, with the consensus being that vendors should pay and include the costs of assessment in the unit costs of their solutions. The pros and cons of each option are laid out here:

EXHIBIT 23

	Payment options	Pros	Cons
PREFERRED	Vendor pays	<ul style="list-style-type: none"> Market pays once for assessment Costs can be included in the unit price of the goods and evenly spread over customers Vendors will bring products to market when they are confident of their efficacy 	<ul style="list-style-type: none"> Vendors may see it as an additional tax on their business Risk of profit incentive for assessors, potential to lower assessment rigour to attract more vendors
	Buyer pays	<ul style="list-style-type: none"> Avoids a financial relationship between vendor and assessor 	<ul style="list-style-type: none"> Market pays multiple times for the same assessment Provides an incentive for buyers to consider fewer products
	Sector association pays	<ul style="list-style-type: none"> Avoids a financial relationship between vendor, or buyer, and assessor 	<ul style="list-style-type: none"> Allocation of costs per buyer in the sector is hard to share fairly Requires additional work to coordinate
	Vendor and buyer pay	<ul style="list-style-type: none"> Provides balance of financial relationships between vendor, buyer and assessor 	<ul style="list-style-type: none"> Market pays multiple times for the same assessment

In the event that a 'vendor pays' model is selected then varying 'depths' of assessment report could be used. For new vendors without scale then a shallower (and therefore cheaper) assessment could be accepted by the market, whereas, for established vendors who already have scale, deeper assessments would be required. When tested in the cohort interviews the idea of 'bronze, silver and gold' depths of assessment was accepted at a high level.

The second issue relates to assessment dispute and how to minimize disagreements. Through interviews with assessment organizations it became clear that this is a real challenge. From the assessor perspective, any assessment requires the full trust of the vendor if it is to be accepted. As one assessor put it, "the evaluation approach needs to be public so it can be replicated. It has to have the strength of a scientific paper for it to be trusted."



Potential disputes could arise when vendors disagree with assessments, or assessors fail to get the required transparency and cooperation from vendors, or even if buyers disagree with the assessment. In terms of the solution, this is where regulators may need to play a role to define dispute resolution mechanisms and the standards that apply to assessment organizations, vendors and buyers.

Assessment standards and organizations

Many interviewees highlighted the need for standards to cover the assessment process and would even go so far as to say that regulation may be needed to effect change (40% of CISOs in the cohort proactively mentioned regulation as being required, and interestingly, so did 25% of vendors). The key is to make the standards effective and sustainable, hence the focus on assessment standards rather than technology standards. In this way assessment standards would be used by regulators to assure the quality of accredited assessor organizations. Such standards will need to be developed jointly by all stakeholders, including regulators, vendors, assessors and buyers. As previously noted, the idea of cybersecurity ratings and assessments is not a new one. Gartner commented in 2018, “by 2022, cybersecurity ratings will become as important as credit ratings when assessing the risk of business relationships.”²¹

Through the interviews it was possible to identify some important principles for assessment that will be required to make the new model work:

EXHIBIT 24

Assessment principles	Details
 DEEP based on detailed analysis of design and implementation	Given the complexity of individual technologies and their integration each efficacy assessment demands very detailed work by highly qualified people, in some cases requiring up to more than a year's worth of work to fully analyze. This also requires strong cooperation from the vendor
 FLEXIBLE to cope with innovation and market structure	Given the high rate of innovation in both security products and the systems they are trying to protect then the approach needs to be able to absorb those changes and enable comparison over time
 RISK-FOCUSED needs to inform buyers	Given that buyers don't have the time to be expert in all technologies they need information to support a risk-based decision on whether to progress with a solution, assessment is not 'yes or no' but more graded and nuanced, there being no single, right, answer
 TRANSPARENT to help increase trust	Given the incentives involved, efficacy assessment needs to be high trust and allow buyers to validate vendor claims and assessor capabilities. Assessment needs to respect vendors' needs to protect their IP while not allowing them to use this to prevent suitable assessment (e.g. use anti-reverse-engineering clauses to discourage vulnerability analysis), may need new legislation
 COMMONALITY to allow multiple assessors in the market	Given the scale of the task and the potential need for specificity per sector then many assessor organizations are required, maintaining commonality of assessment standards is therefore key

²¹ Gartner, “Innovation Insight for Security Rating Services”, Sam Olyaei, Christopher Ambrose, Jeffrey Wheatman, 27 July 2018

These principles can be made more specific by considering what standard to aim for in assessment against each element of the efficacy of cybersecurity technology definition. Here we lay out some examples of those standards and aims that respond to the concerns of the cohort:

General assessment standards

- Assessments should be conducted by personnel with recognized levels of technical skills, as with red team testing (already semi-regulated and standardized, eg, CREST)
- Vendors need to expose the “how” not just the “what” of their products so that it is a “white box” assessment not “black box” assessment (clearly appropriate confidentiality controls will be needed to avoid vendor intellectual property loss)

Capability standards

- Solutions that allow verification of all vendor claims on capability. For example, by exposure to known attacks and by operation in test environments to assess whether products will be effective against future, as-yet-unknown attacks
- Security vendors need to provide clear information of what their products should do and the expected limits of their capabilities, for example, including clearly documented Security Targets that link explicitly to marketing claims

Practicality standards

- Solutions with relatively few integration, operational and maintenance issues. Aiming for ‘install and go’ (can be tested in various industry-specific archetypal operating environments)
- Security products designed on the assumption that users make mistakes
- Security products that require complex configuration changes before they become vulnerable, rather than requiring complex configuration to be secure
- Solutions that fit into architectural patterns that assume realistic limitations of real-world products and implementations rather than assuming perfect products and operations
- “Protect” security products designed to enable effective monitoring of their operation and performance
- Security products that engender confidence by making security audits easy

Quality standards

- Security products that themselves have low levels of vulnerability based on build quality and security architecture
- Security products that “enforce good” rather than “detect bad”
- Security products designed to support detailed analysis and testing of their capabilities and vulnerabilities as opposed to analysis and testing only of their design ambitions

Provenance standards

- Enterprise security maturity of the vendor
- Full transparency of the supply chain of the vendor

The above standards are intended purely as a thought starter: the cohort fully realized the additional depth of work that would be required to set assessment standards. However, having observed the approaches adopted by the GSMA in the Security Assurance Scheme²² (where standards are set on the capabilities of the assessment organizations, and are strong enough to drive real change), we are confident that a solution can be found.

²² <https://www.gsma.com/security/security-accreditation-scheme/>

With assessment standards in place the current frameworks for cybersecurity maturity could also be modified to take account of the need to assure technology efficacy. For example, for either the CQUEST or NIST current assessments, simple changes could be made as per the below exhibit:

EXHIBIT 25

Opportunity	CQUEST current text	NIST current text	Proposal
1	Qu. 13: Are hardware and software vulnerabilities proactively identified and documented with their risk assessment?	Identify: Risk Assessment: ID.RA-1: Asset vulnerabilities are identified and documented	Could explicitly include the requirement for security solution efficacy assurance, currently this is a very broad requirement about gathering all risk information relating to the assets
2	Qu. 23: Do you have effective processes and procedures in place to assess the security capabilities and management of cyber risk by third party providers?"	Identify: Supply Chain: ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Could explicitly include assurance of the actual products and services the supply chain is delivering (especially the security solutions)
3	Qu. 28: Do you employ multiple layers of security to ensure that the corporate network is segregated effectively and protected from externally facing systems (e.g. firewalls and multiple AV vendors)?	N/A – no comparable clause	Could consider clarifying the statement 'the organization does not rely on a single solution for any of its cyber defences' in the context of solution efficacy assurance
4	N/A – no comparable clause	Protect: Information Protection: PR.IP-8: Effectiveness of protection technologies is shared	Need to explain how protection technology effectiveness is measured, as well as shared. Also, the ISO text focuses on learning from incidents where effectiveness is better understood, so this text could also be modified to add in a focus on learning from testing of effectiveness

"Using NIST maturity assessment questions to drive a greater efficacy focus could work given the compliance requirement and the current scale of adoption"

Travel industry CISO

CYBERSECURITY TECHNOLOGY EFFICACY IS CYBERSECURITY THE NEW “MARKET FOR LEMONS”?

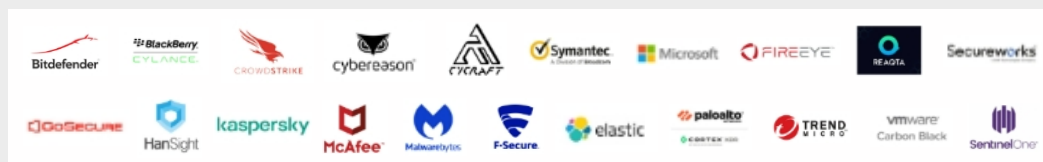
In terms of standards implementation, we have already seen a good example of independent product assessment by MITRE Engenuity, such as the APT29 test. The success of this scheme is in part due to the strong collaboration from vendors to make it work, that contribution is valuable and critical to the success of any scheme...

EXHIBIT 26

HOW DID THE TEST WORK?

In late 2019, the ATT&CK Evaluations team evaluated 21 endpoint security vendors using an evaluation methodology based on APT29.

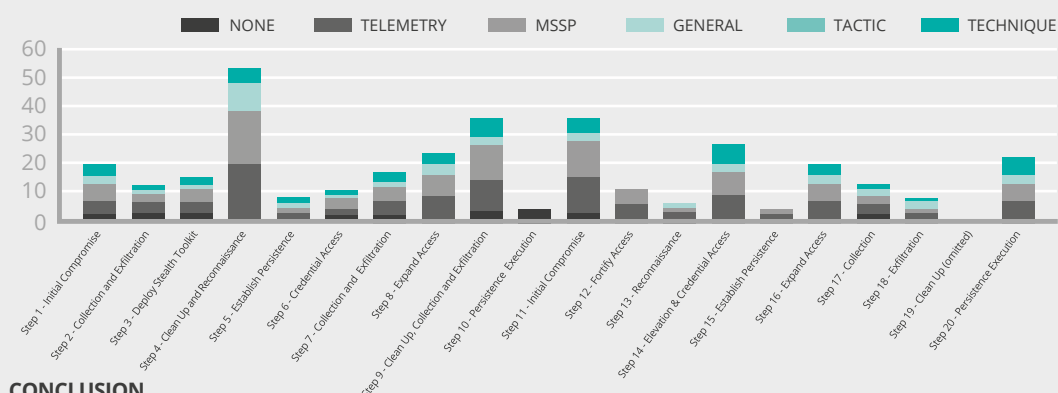
This was already a publicly known attack, so the vendors had the opportunity to prepare for the test.



WHAT WAS TESTED?

The results comprise a robust dataset of recorded detections, mapped to ATT&CK, that enable users to make informed decisions on what tools meet their needs, as well as how to improve detection capabilities of their current deployments. The results do not provide a score or ranking of the participants. There was no winner.

MITRE tests the security products functionality in comparison with other products under the same attack, testing 'how well does it do security', not penetration testing the product itself.



CONCLUSION

MITRE is moving in the right direction in terms of creating information transparency on solution efficacy. The next step would be to broaden and deepen the test to cover the full definition of efficacy.

SOURCE:
<https://attackevals.mitre.org/APT29/>

To implement the standards would require growth in the 'assessment base' of organizations with the capability to assess. Here is a selection of the types of organization already active in this space:

- **MITRE ATT&CK Evaluations:** evaluates cybersecurity products using an open methodology based on the ATT&CK® knowledge base
- **NSS Labs:** independent assessment company, buyer pays for reports
- **Common Criteria labs:** available in a number of nations, however, suffering some fragmentation across international lines
- **ISA Secure:** not for profit, industrial automation and control security certification (includes organizational certification), vendor pays for certification test
- **NIST / CQUEST:** organization focused assessment of company maturity, requires 3rd party audit
- **Spirent:** global provider of automated test and assurance solutions for networks, cybersecurity, and positioning
- **NCC Group / @Sec:** providing assurance to the telecoms industry and others as required
- **ISCA Labs:** independent assessment company, part of Verizon, vendor pays for certification test

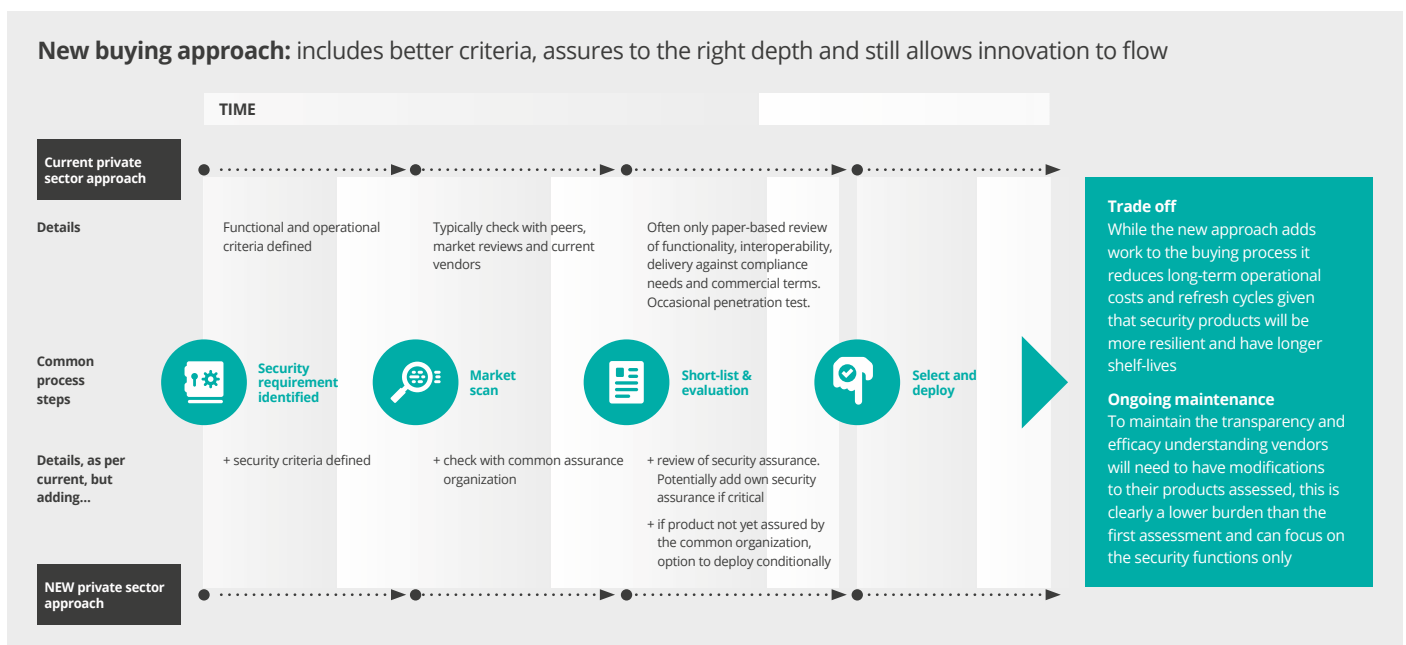
Clearly the implementation of new standards and transparent assessments would be a challenge for the industry. However, given the momentum that is already building around information sharing and common transparency, we are confident that change can be delivered. For example, common transparency is already being delivered in some of the following ways:

- **ISACs:** Information Sharing and Analysis Centers, typically sector focused, eg. FS-ISAC for financial sector, for 20+ years. Focus on sharing threat intelligence
- **TIBER-EU:** threat-intelligence based ethical red-teaming framework working across the European Union (CBEST is the UK equivalent), established 2018
- **Cyber Threat Alliance:** started in 2015, a sharing and collaboration platform for security vendors on threats and indicators of compromise (IOCs)
- **ISACA:** professional credentials for individuals
- **CREST:** accreditations for organizations and professional level certifications for individuals
- **NTIA SBOM:** initiative to create transparency on software componentry and sourcing
- **Telecoms:** has various bodies sharing standards and assessments, eg. GSMA / ETSI, GCF, 3GPP
- **Consumer Product Security:** for example, the UK government consultation on regulation is underway (June 2020)

Better buying

All previously mentioned changes to the system and capabilities should lead to an improved buying process in the enterprise. The buying process should benefit from better criteria for selection and assurance to the right depth while still allowing for innovation. Ideas around common approaches to understanding technology efficacy are not new, as was identified in some joint research between McKinsey and the IIF in April 2020²³ where 40% of respondents said they would be willing to undertake joint third party and vendor due diligence. There was also mention of cyber certifications and joint initiatives to improve operational resilience of the ecosystem. Considering all the inputs received in the study it is possible to propose a new buying process as per the below exhibit:

EXHIBIT 27



²³ <https://www.mckinsey.com/business-functions/risk/our-insights/the-cybersecurity-posture-of-financial-services-companies-iif-mckinsey-cyber-resilience-survey>

Vendor perspective

While the proposed changes to the economics of the cybersecurity market add a burden to the vendor, they will also help open up the market for them. Those that can bring the best technology will be better able to get traction in the market.

Two possible challenges to consider from the vendor perspective are how much potential there is to really bring better technology to market and whether it will prove economically and operationally feasible to use higher specification security solutions in the private enterprise market.

In terms of the potential to bring better technology to market, the interviewees were broadly confident that vendors could meet the challenge, with one remarking that “some vendors see that the more secure products don’t sell well, so security engineers work on ‘sell-able’ products instead of working on effective products, so actively reducing the security efficacy”. Given recent increased transparency from government agencies sharing novel security architectures we are confident that technology development can progress. The exhibit below shows two examples from the UK National Cybersecurity Centre (NCSC):

EXHIBIT 28

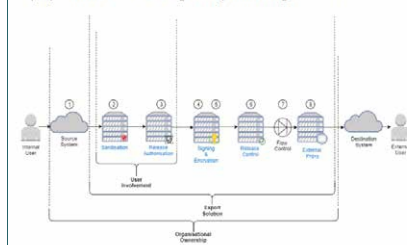
UK NCSC is sharing approaches that can be used in enterprise

Example 1: end to end export solutions:

“Most organizations need to communicate externally, passing data across organizational boundaries. However, enabling this process, without also risking the leak of sensitive data, can be difficult.

This guidance provides an architecture pattern which will help you to share data, while maintaining the security of your core networks and systems.”

A proposed end-to-end design is depicted in Figure 1. below.

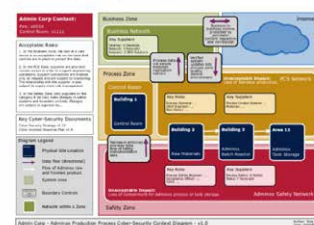


Example 2: design principles and Operational Technology:

“If you are responsible for the design or maintenance of an Operational Technology (OT) network, this study will help you to navigate the cyber security issues you will encounter as you design your cyber-physical system.

Having established some of the fundamental aspects of the system, Admin Corp will then generate, communicate and agree upon a simple diagram of the plant, that depicts and end-to-end understanding of the physical process and logical network design”

A simple network diagram
The Adminox system diagram could look like this:



SOURCE:
<https://www.ncsc.gov.uk/>

To identify whether highly performing security technologies can be feasible both economically and operationally, we looked at the cross-over between secure government and the private sector. In theory if a secure government organization has selected a solution then it should be highly effective. If that solution is also successful in the private sector, so then the economics of development are feasible. To that end we observe two levels of assessment and solution implementation in the government space.

First, there is a Basic Assessment level, an example of which is the US NIAP:

- US National Information Assurance Partnership (NIAP) is run by the NSA and oversees a national program to evaluate Commercial Off-The-Shelf (COTS) Information Technology (IT) products for conformance to the Common Criteria
- Successful evaluations benefit industry product developers/vendors and government procurers by validating that the products meet security requirements for U.S. national security system procurement
- While this program does provide a level of assurance about solution efficacy it doesn't necessarily include full assessment of efficacy as defined previously in this report, typically only working to Common Criteria EAL1 or 2
- Many of the major names in technology and security have products approved on this list

Second, there is a Fuller Assessment level, which gives us confidence that even at the highest levels of security efficacy there is an economic solution to serve the private sector. Some of the key points around Fuller (or High Assurance) are:

- For the most secure environments, higher levels of testing and assurance are undertaken, typically based on standards that are not shared publicly. Our view is that the private sector should be moving towards (but not necessarily meeting) these higher standards of assurance.
- Examples of vendors in the most secure environments that also serve the private sector (often with variants of solutions) include Airbus, BAE Systems, Deep Secure, Forcepoint, Garrison²⁴, Owl Cyber Defense, Raytheon, Trident, Ultra Electronics, etc.

Given companies that serve both secure government and private sectors are able to gain access to this market, we are confident that vendors will be able to produce commercially viable solutions that meet a higher bar of efficacy if they are incentivized to devote more investment into solution development.

²⁴ Note: Garrison funded this research

**4**

CHANGING MARKET INCENTIVES WILL REQUIRE CONCERTED EFFORT ON THE BUY-SIDE

Delivering a new model will require coordinated action on the part of buyers to change the market incentives by demanding efficacy transparency before they trust technology. This approach should remove the first-mover disadvantage and unlock the situation. Clearly vendors, assessors and standards setters (typically industry associations or regulators) will also need to play their part in delivering the change, but if buyers create the demand the incentive will exist to do so. The idea of independent transparent technology assessment is not new, but there is little incentive for it in the commercial market today: this study suggests that the time may be right to revisit how this can work. The findings of this work may prompt new questions and debates within organizations and the wider market, some of which will be challenging discussions given the issues identified. However, every effort has been made to give a fair representation of the cohort's views and the intention of this report is to be a catalyst for improvement of the industry and better outcomes for all parties.



Proposal for buyers

(including all in the enterprise, eg. CISOs, CIO, procurement etc.)

Actions to consider include:

Demand transparent assessment of efficacy:

- Adjust procurement approaches to demand transparency on solution efficacy from vendors
- Work with industry associations and regulators to create coordinated agreements demanding efficacy assessment (going deeper than current broader pushes for questionnaires and basic attestation, and creating new market incentives)

Support efficacy and assessment improvement:

- Increase the profile and assessment of cybersecurity efficacy with all partners
- Engage with vendors to support development of more effective solutions
- Engage with assessment organizations and leverage their services

Build Internal capability:

- Increase internal understanding of security efficacy and the options for differentiated outcomes



Proposal for vendors

Actions to consider include:

Deeper buyer engagement:

- Work with customers to provide transparency on solution efficacy

Support common assessment:

- Support (sector) efforts to expand common assessment capacity and create approaches they can trust

Raise standards:

- Work with sector assessment and regulatory bodies to implement greater focus on technology efficacy

Shift investment strategy:

- Rebalance investment from marketing towards developing cybersecurity solutions with greater efficacy



Proposal for assessors

Actions to consider include:

Expand common assessment:

- Look at how to expand common assessment capacity for the sector companies to leverage

Embed efficacy definition:

- Look at how to include technology efficacy in sector standards and assessments for cybersecurity, in a way that vendors can support

Increase education and collaboration:

- Share knowledge with sector companies, sector associations and regulators to promote the concept of cybersecurity efficacy and best practices



Proposal for regulators

Actions to consider include:

Expand common assessment:

- Work with each sector to define an approach to common assessment that can be trusted by all stakeholders

Develop standards definitions:

- As required, create standards for the assessment of cybersecurity technology efficacy

Promote education and collaboration:

- Share knowledge with sector companies, associations and regulators to promote the concept of cybersecurity efficacy and best practices



5

RESEARCH METHODOLOGY

The author of this research is Joseph Hubback (working as an independent consultant) and it is published by Debate Security (an independent group that brings together industry experts to talk about the cyber market and how it can be improved). Garrison Technology funded Hubback's time while all interviewees contributed on a voluntary basis. The interviews for this research have been conducted independently from the sponsors of the work, and while the sponsors have helped with problem solving and analysis, editorial control has remained with the author.

Interviews

All interviews were all conducted one-on-one, on a confidential and non-attributable basis. This approach was adopted to encourage candid responses. The set up and questioning approach has been designed to avoid bias and where there has been risk of bias this has been explicitly discussed in the interviews. Each interview lasted at least 30 minutes with most lasting around an hour and many leading to follow-up conversations to discuss the conclusions of the research.

Cohort

The cohort of interviewees were approached based on their depth of expertise and were selected to build a balanced set of inputs. The roles covered in the cohort include CISOs (around 50% of the whole group; coming from globally leading institutions, Fortune 500 companies and elite government environments), cybersecurity vendors, technology vendors, enterprise leaders (Chairs / CEOs), assessment organizations, government agencies and industry associations or regulators. Financial services is the most strongly represented sector, while input has also come from telecoms, aerospace and defense, health, legal, automotive, logistics, travel, industrial and retail sectors. Geographically the interviewees most commonly hold global roles (>50% of people) so have broad perspectives, the rest of the roles covered US, European or country specific areas. Most respondents were based in the UK and US but many were based in other countries too (typically European).

Review

The interviewee cohort has been given the chance to review intermediate drafts and this final report before publishing. Detailed feedback has been received from a number of them.

Acknowledgments

The author would like to thank all the interviewees for their input and time, without which this research would not have been possible. Special thanks also go to Robert Rodriguez for his support in setting up many of the interviews. The following interviewees have given permission to be named:

Interviewee	Role
Aernout Reijmers	CISO
Allan Friedman, PhD	Director, Cybersecurity Initiatives, NTIA, US Department of Commerce
Andrew Rose	CISO
Bernard Parsons	CEO, Becrypt
Bob Gourley	CTO, OODA LLC and former CTO, DIA
Brian Geffert	CISO
Carolann Shields	Former CISO, KPMG
Ciaran Martin	Former CEO, NCSC
Craig Rice	Director of Cyber Resilience
Dan Turner	CEO, Deep Secure
Dave Larson	Security Expert
Professor David Fairman	Deakin University and former CISO & Security Expert
Donna Dodson	Former Fellow and Cybersecurity Advisor, NIST
Sir Douglas Flint	Chairman
Duncan Greenwood	Vice President & General Manager, NEMEA, VM Ware
Frank Duff	Director of ATT&CK Evaluations, MITRE Engenuity
Gerald McQuaid	Security Expert
Haydn Brooks	CEO, Risk Ledger
Homaira Akbari	AKnowledge Partners
Ian Glover	President, CREST
James Chappell	Co-Founder, Digital Shadows
James Hatch	Chief Digital Officer, BAE Systems Applied Intelligence
James Kaplan	Partner, McKinsey & Company
James Moran	GSM Association
Jamie Saunders	Security Expert
Jay Gonzales	CISO
Jean-Yves Poichotte	CISO
Joe Sullivan	CISO
John Cryan	Chairman, Man Group and former CEO, Deutsche Bank
John Noble	Security Expert
John Rogers	CISO
Jonathan Lloyd-White	CISO

Interviewee	Role
Laura Deaner	CISO
Mark Settle	Author and former CIO, Okta
Martin Whitworth	Security Expert
Mike MacIntyre	VP of Product and Co-Founder, Panaseer
Paddy Francis	CTO, Airbus Cybersecurity
Patricia Muoio	General Partner, SineWave Ventures
Paul Crichard	Chief Security Technology Strategist, BT
Rob Bening	Retired CISO
Rob Dartnall	Head of Intelligence, Security Alliance
Rob Newby	Founder, CEO and CISO, Procordr
Robert Rodriguez	Chairman and founder, SINET
Robert Coles	CISO, Cumberland House Consulting Ltd.
Santosh Chokhani	Security Expert
Shaun Khalfan	CISO
Simon Reiniche	FS-ISAC
Simon Riggs	CISO
Stefan Lueders	Computer Security Officer, CERN
Steve Zalewski	CISO, Levi Strauss & Co
Thomas Maillart	PhD, Security Expert, University of Geneva
Tim Orchard	EVP Managed Detection and Response, F-Secure
Tucker Bailey	Partner, McKinsey & Company
Wim Hafkamp	Managing Director, Z-Cert and former CISO

References

- 1 <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>
- 2 <http://reports.weforum.org/global-risks-report-2020/appendix-b-methodology/>
- 3 <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>
- 4 <http://reports.weforum.org/global-risks-report-2020/appendix-b-methodology/>
- 5 Crunchbase
- 6 <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>
- 7 Accentue, Ninth Annual Cost of Cybercrime Study, 2019
- 8 Accentue, Ninth Annual Cost of Cybercrime Study, 2019
- 9 <http://reports.weforum.org/global-risks-report-2020/appendix-b-methodology/>
- 10 <https://www.jstor.org/stable/1879431?origin=JSTOR-pdf>
- 11 https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/ts090310_lewis.pdf and <https://obamawhitehouse.archives.gov/files/documents/cyber/Congress%20-%20031009%20HHS%20ETCST%20Cybersecurity%20Transcript.pdf>
- 12 SOURCE: Club CISO Report 2020
- 13 <https://www.zdnet.com/article/average-tenure-of-a-ciso-is-just-26-months-due-to-high-stress-and-burnout/>
- 14 <https://www.clubciso.org/downloads/>
- 15 <https://www.mckinsey.com/business-functions/risk/our-insights/securing-software-as-a-service>
- 16 <https://momentumcyber.com/docs/CYBERscape.pdf>
- 17 <http://petercohen.me/>
- 18 <https://www.cbronline.com/news/ransomware-2019>
- 19 <https://viterbi-web.usc.edu/~shaddin/cs590fa13/papers/AkerlofMarketforLemons.pdf>
- 20 <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>
- 21 Gartner, “Innovation Insight for Security Rating Services”, Sam Olyaei, Christopher Ambrose, Jeffrey Wheatman, 27 July 2018
- 22 <https://www.gsma.com/security/security-accreditation-scheme/>
- 23 <https://www.mckinsey.com/business-functions/risk/our-insights/the-cybersecurity-posture-of-financial-services-companies-iif-mckinsey-cyber-resilience-survey>
- 24 Note: Garrison funded this research

RESEARCH REPORT
**CYBERSECURITY
TECHNOLOGY
EFFICACY**

Is cybersecurity the new “market for lemons”?