Global Information Assurance Certification Paper

Crossing the line:
Joining forces with your customers

GIAC Information Security Fundamentals Gold Certification

Author: Jules Vandalon,vandalonja@gmail.com
Advisor: Stephen Northcutt
Accepted: February 23, 2016

Template Version September 2014

Abstract

When it comes to information security, customers trust you to protect their personal data when doing business with you. So you invest heavily in upgrading hardware, software and in improving security measures within your organization. After all, trust is the essential element of the customer relationship. But how do your customers react when you tell them that one of their devices has been infected by malware? Or when you help them to meet a certain level of information security?

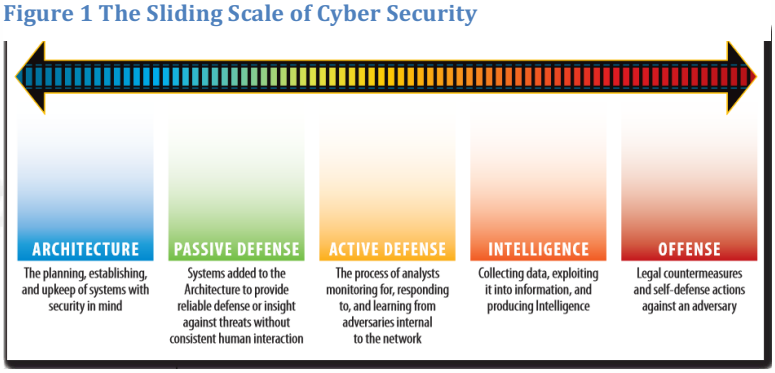
Information security is a shared responsibility between a company and their customers. But where do you draw the line? This paper assesses where the line can best be drawn. It does this by examining the pros and cons of three models: Split responsibility, Joint responsibility, and Full responsibility. It argues that Joint information security can create a competitive advantage that, in the end, creates and sustains a better information security and a better performance of your organization in comparison with the other two models.

1. Introduction

Anyone who starts in the field of information security quickly gets familiar with setting up a secure architecture, setting up defense mechanisms and much more. Due to research done on effective measures by security experts, and experience with these measures within the security field, it is known what measures prove to be effective and useful. Examples of these measures can be found in the Critical Security Controls of the Center for Internet Security (CIS). A set that provides specific and actionable ways to defend oneself based on the experience of a broad community of government and industry practitioners (SecurityControls, 2015). Another model to get an overview of the field of information security is 'The Sliding Scale of Cyber Security ' (Lee, 2015). The model consists of five categories: Architecture, Passive Defense, Active Defense, Intelligence, and Offense.

Lee succeeds in setting up a framework by which to understand actions contributing to cyber security and which can be used to measure the security maturity of an organization.

Figure 1 The Sliding Scale of Cyber Security



Four out of five categories are aimed at the internal organization. And the one, that is crossing the line of the organization, is Offence. Lee states: "civilian organizations cannot currently participate in such actions and remain within the spirit of the law." (Lee, 2015). And therefore, Offence cannot be used at this time. This conclusion is supported by another paper on this subject: "To urge a risk-based approach to use even lawful active defense tactics would be to state the obvious, and the use of certain types of active defense where misattribution is possible, may be to entirely abandon the risk-based approach to problem-solving." (Harrington, 2014)

What has not yet been explored is joining forces with your customer. For this purpose, I have added a sixth category to Lee's model, called Allies. This name is chosen to keep it in line with the vocabulary Lee has chosen to use in the field of cyber security.

Jules Vandalon, vandalonja@gmail.com

It contains actions contributing to cyber security of the own organization in relation to other entities such as; customers, strategic partners, suppliers, competitors and regulators that join in an Alliance for mutual benefit within the information security field. This new category should be placed between Intelligence and Offense on the right-hand side of the scale. Lee proposes to first build the categories on the left-hand side of the scale to build a solid foundation; Architecture, Passive Defense, and Active Defense. It creates a proper return on investment and makes the actions on the right-hand side obtainable. Allies should come before Offense because that is not (yet) obtainable. Allies should be placed after Intelligence because of the relationship between them. Data coming from Allies can be exploited into information by Intelligence to feed Active Defense. An example is the sharing of Indicators of Compromise (IOC) between Financial Service Providers in Europe. The intelligence department of an FSP translates these IOC's into rules to apply on, for example, the click stream coming from their customers. The FSP is actively hunting for malware on the devices of its customer and is acting proactively on the threat landscape.

Forming an Alliance with suppliers, regulators, and branch organizations is not a new idea. It has often been promoted in the past, e.g. by the World Economic Forum in 2012 (WEF, 2012). Forming an Alliance with your customer seems to be an unexplored idea. It has not been researched in depth. Only two papers can be found on the subject. The papers are: (Begum, 2008) about the relation between security and privacy and customer adaptation of electronic banking. And (Dommelen, 2013) about Financial Service Providers joining forces with their customers in order to mitigate the likelihood of successful attacks on the customer's online banking account. It also is not part of the Critical Security Controls, nor is their mention of it in the model promoted by the WEF.

This paper is limited to the customer part of Allies. It would be going too far for this assignment to deal with the whole spectrum of the category. Does joining forces with your customer constitute as an effective measure? And if it does, what is the best participatory model? In order to determine this, the sliding scale of responsibility is examined, from Sole responsibility with the organization to Split responsibility to Joint responsibility to finally Sole responsibility with the customer. The paper deals with the advantages and disadvantages of the following categories:

- Full responsibility: Provide the customers with a total solution that works automatically and without issue. The supplying organization assumes full responsibility. None with the customer. No cooperation is needed.
- Split responsibility: Both the organization and the customer are each responsible for their own information security. No responsibility is shared. There is no cooperation and no sharing of resources, information or other measures were taken. The liability of the organization goes as far as the border router.
- Joint responsibility: Both the organization and the customer are responsible for their own information security and are willing to cooperate within the security field. Information is shared. Resources made available for customers. There is cooperation.
- The model where all responsibility rests solely with the customer is not part of this paper. It is impossible for an individual customer to implement and is not in accordance with the law and is dropped beforehand.

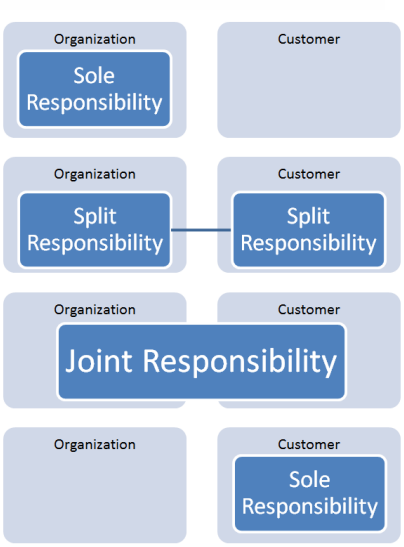


Figure 2 Sliding scale of responsibilit

On the basis of the analysis, the best option becomes apparent. A recommendation is made where the line should be drawn in the best interest of security, continuity and sustainable performance of the organization.

2. Business Strategy Decision

Before an organization can make a choice for one of the three categories, management has to have a clear view of the pros and cons. It involves altering the Business Strategy in a fundamental way.

Academics and managers have developed numerous models to assist in this decision-making process. One of those models is the PESTLE model. PESTLE analysis is in effect an audit of an organization's environmental influences with the purpose of using this information to guide strategic decision-making. Similar acronyms are SLEPT and PEST.

Morrison describes it in chapter 3 of his book, where he sets out the practical application of this diagnostic approach. (Morrison, 2013).

The PESTLE acronym stands for Political, Economic, Socio-cultural, Technological, Legal, and Environmental. Its true history is difficult to establish because it has not been claimed, nor has it been copyrighted. The PESTLE model demands to put the organization in the environment in which it operates. Normally the country where it does business is chosen. This analysis of this paper is performed within the context of Dutch society with all its aspects.

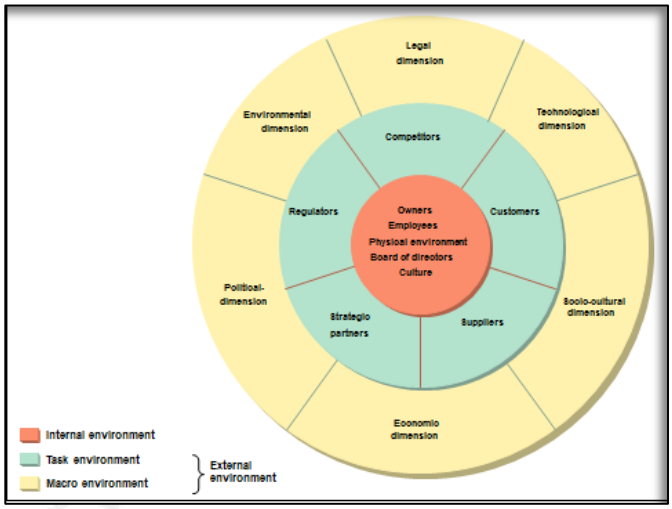


Figure 3 Pestle Model: Know where you are now and where you want/ need to be

2.1. Securing your Customer

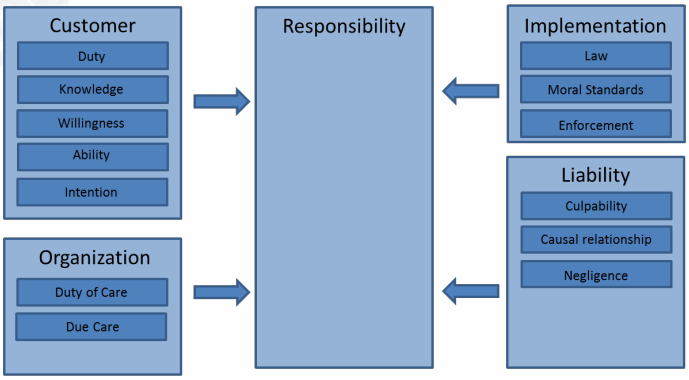
Traditional PESTLE model uses factors of a general level. This paper is about information security in relation to the customer and about responsibility. For each category, we need to explore the factors that influence information security, the customer, and responsibility. We start with exploring the concept of the Customer. There are many different studies done on the behavior of customers. They try to understand the processes customers use to select, secure, use and dispose of products, services, experiences, or ideas (Kuester, 2012). This is done in order to predict the behavior of customers.

If an organization is able to do so, it can seamlessly align with customers' needs so that the continuity of the organization is guaranteed. Customer behavior blends elements from psychology, sociology, social anthropology, marketing, and economics. Security and Privacy are elements that play a role in the customer behavior. (Barnes, 2007). To be precise, lack of privacy and security were found to be significant obstacles to the adoption of, and a positive attitude towards a product. A study done into the role of perceived security and privacy on customer adaptation in the context of electronic banking supports this claim (Begum, 2008). They found that Security and Privacy have a positive effect on customer attitude and a positive effect on customer adaptation.

There is no recent research. This poses a problem, in that in the last 8 years between the research of Begum and now, there has been a major shift in the use of devices, applications, the introduction of the Internet of Things, etc. And with that change, comes a change in the attitude and adoption of technology. This, in turn, has an influence on the (perceived) security and privacy of customers of a product. Although no conclusive scientific evidence can be delivered, it stands to reason that both (perceived) security and privacy are of significant influence on customer satisfaction. A company that is able to provide both elements is able to create a competitive advantage and with that, a better performance of the organization.

Next to the customer, responsibility plays a role when examining the alternative of Split-, Joint- and Full responsibility. There are multiple elements that are conditional for responsibility. To paraphrase the model constructed by Dommelen (Dommelen, 2013). On the organization side, we have Duty of Care and Due Care. On the Customer side, we have the elements of Duty, Knowledge, Willingness, Ability and Intention. On the other side, we have Laws and regulations and a Moral standard and the Enforcement of those laws and regulations. And the fourth category is Liability that consists of Culpability, Causal relationship, and Negligence. The elements mentioned in this paragraph on the customer and responsibilities are put within the context of the PESTLE model on the next pages.

Figure 4 Responsibility Model Dommelen 2013



2.1.1. Political dimension

In a traditional PESTLE analysis, the political factors include government attitudes to employment, consumer protection, the environment, etc. Here the Dutch factors regarding cyber security in relation to the customer and responsibility are discussed. The Dutch government is in favor of a digital society, as this creates important benefits for the Dutch country, their citizens, and Dutch companies.

Safeguarding digital security and freedom and maintaining an open and innovative digital domain are preconditions for the proper functioning of such a society. The general point of view of the Dutch government is that they have a limited task in the area of business to consumer, in the sense of legal regulation. The government is only willing to impose laws and regulations in cases of serious physical or financial risks for the customer. The majority of tasks related to consumer protection are normally delegated to the deliberation between the consumer organizations and the manufacturers (Raaij, 1997).

Where consumer protection specific for the digital economy is concerned: this brings new knowledge, risks and responsibilities with it. In the Cyber Security Strategy document (NCSS 2, 2013); the Dutch government states that security is a core task of the government, also in the cyber domain. It also states that the government has a responsibility to enhance the online security and privacy of their citizens. "The Dutch government commits itself to increase the cyber security awareness of their citizens, companies and governments, to counter cyber criminals and to prevent social disruption due to cyber incidents. If necessary, the government will impose rules, regulations and standards" (page 19, (NCSS 2, 2013)).

When it comes to responsibility, the standpoint is somewhat ambiguous. On the one hand, the Dutch Government states that "we can't expect our citizens to completely understand and assess the security and privacy aspects of the increasing complex ICT services and products offered by large international companies. There is a clear responsibility for these companies to take care of the customer's security and privacy. They need to be transparent about their efforts and measures for enhanced cyber security". On the other hand, the government is of the opinion that "we could expect a certain level of basic cyber hygiene and ability of citizens using IT devices. For example, being careful with personal information and using strong passwords" (page 20, (NCSS 2, 2013)). The Netherlands are part of the European Union, a political-economic union. There are rules and regulations from the EU that apply to the Netherlands. For the field of cyber security, the European Parliament adopted a proposal for a Network and Information Security Directive (NIS Directive).

The directive is part of the European Union's Cyber Security Strategy aimed at tackling network and information security incidents and risks across the EU. It consists of five main elements: 1. National strategy, 2. Take part in a co-operation network, 3. Set security requirements, 4. Make use of standards and 5. Enforce those requirements and standards. The NIS Directive will require many businesses to demonstrate that they make effective use of these security policies and measures. Failure to do so may result not only in the loss of customer trust and damage to reputation but also breach European data requirements and trigger enforcement actions or liability claims. (European Commission, 2015).

In conclusion, we see the public sector working together with the private sector on a national and international level. Joining forces and tackling the cybersecurity threats in order to make full use of the commercial and socio-cultural benefits. The political dimension does not accept a Split responsibility model. The politicians in Europe and the Netherlands see a clear responsibility for all parties involved. And if the private sector does not take this responsibility seriously the government will step in and take action. The Joint responsibility alternative corresponds with the current vision of cyber security course of the government and the EU and is acceptable. The government and EU do not mention customers as an active partner. Customers are mentioned as a passive party that needs protection. The Full responsibility alternative has not been implemented anywhere. An implementation that comes close is the one of the Apple Corporation. Apple has almost full control over their value chain. Apple, however, does not take full responsibility. Part of the responsibility and liability is put on the customers. With this implementation in mind, we can theorize. It stands to reason that the attitude of politicians towards the Full responsibility alternative is neutral to positive. As long as customers can do their business without risk or incidents and keep their faith in the products involved and the in the digital society, this alternative is acceptable.

2.1.2. Economic dimension

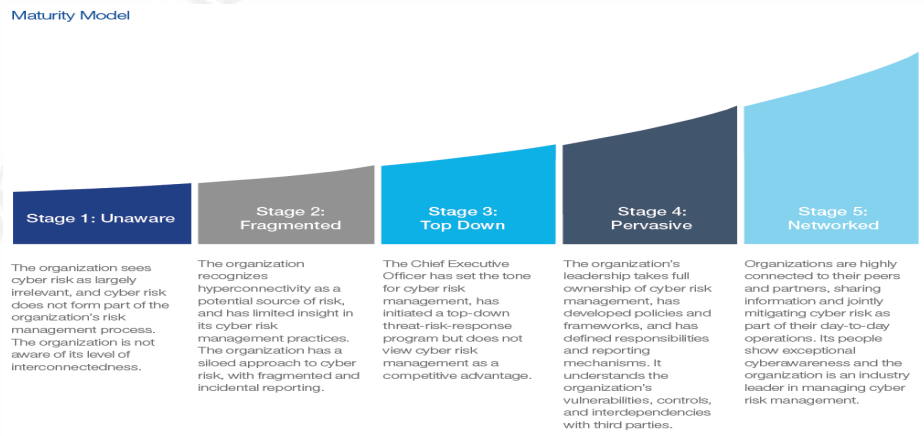
In a traditional PESTLE analysis, the economic factors include assessing potential changes to an economy's inflation rate, taxes, interest rate, etc. Here the economic factors of cyber security in relation to the customer and responsibility are discussed.

In 2014, Forbes ranked The Netherlands as the #11 best country for doing business. Forbes used 11 different criteria to rank countries; innovation, red tape, taxes, investor protection, stock market performance, technology, personal freedom, etc. The digital domain has been a part of Dutch society for more than two decades. During this period, information and communication technology has proven to be an important factor in productivity growth and innovative power within the Netherlands.

The Netherlands is the European leader in responding to technological trends and the effective use of ICT tools and skills. The Netherlands is also an international internet hub, has the world's most competitive internet market and has one of the highest numbers of internet users. (NCSS 2, 2013) The yearly report of Central Bureau for Statistic on ICT, Knowledge, and Economy (CBS, 2015) shows a yearly growth of the acceptance, penetration rate and value of the ICT component of the economy and society.

This increasing dependence on connectivity for the normal functioning of society and economy makes the protection of connectivity a critical issue. And as the World Economic Forum states: 'No one organization can resolve this issue by itself and a collaborative, multi-stakeholder approach must be taken; even competitors in a given industry must become partners in the effort to ensure a stable and trusted environment' (page 4, (WEF, 2012)). The WEF advocates building strong Alliances, as their Maturity Model shows, (page 12, (WEF, 2012). They place the Alliance within a value chain and they exclude the customer. In Figure 3 PESTLE model this environment is called task environment: supplier, competitors, strategic partners and regulators. The task environment of the PESTLE model includes the customer.

Figure 5 Maturity Model WEF



Economics of security is a relatively young discipline. One of the first papers is written by Ross Anderson ´Why Information Security is Hard´ (Anderson, 2000). This publication is considered to be the birth of economics of security. Another author within this discipline is Bruce Schneier, who also wrote various articles and blogs around the same time. In the article 'Hacking, the Business Climate for Network Security' Schneier explains why information security eventually will improve and mature: "Enforce liability and everything else will flow from it." (Schneier, Hacking the Business Climate for Network Security, 2004). He writes "But in the real world, network security is a business problem. The only way to fix it is to concentrate on the business motivations. We need to change the economic costs and benefits of security. We need to make the organizations in the best position to fix the problem, want to fix the problem".

Schneier argues that firstly corporations are going to demand better products or otherwise hold the supplier liable. Secondly, he states that security is fundamentally an economic problem. Because businesses approach security as they do any other business uncertainty: in terms of risk management. The solution is to change the cost-benefit-ratio that holds companies back to make a better product. With that businesses are intrinsically motivated to improve. And thirdly he argues that security is a common: and should be treated as such, protected as any other common. By legislating those areas and by making companies liable for taking undue advantage of those commons the security will improve. In his article (Schneier, Economics and Information Security, 2006) he summarizes the key points. ´We generally think of computer security as a problem of technology, but often systems fail because of misplaced economic incentives: The people who could protect a system are not the ones who suffer the costs of failure. The economic considerations of security are more important than the technical considerations.'

Another economic factor that touches upon security and the customer is called the Lock-in effect. "Lock-in" is an economic term for the difficulty of switching to a competing product. A company gains control over (part of) the value chain. An example is the Apple Corporation. It has control over almost the whole value chain. Even decides what customers can and cannot buy. The upside of this way of doing business: it renders control and with control it increases security. Apple has shown this by becoming and staying one of the safest solutions in the market.

Jules Vandalon, vandalonja@gmail.com

Bruce Schneier wrote an article about this phenomenon pointing out the downsides. “With enough Lock-in, a company can protect its market share even as it reduces customer service, raises prices, refuses to innovate and otherwise abuses its customer base.’ (Schneier, Lock-in, 2008) He argues that companies increase their Lock-in through security mechanisms. Examples are patents, copy protection, digital rights management (DRM), code signing or other security mechanisms. And these organizations use security as an excuse and cover up for what they are really after Control. The essay is about the security-versus-privacy debate, a debate about liberty versus control. It illustrates the Lock-in effect and the possible consequences of it. There are boundaries to the Lock-in set by the government and politicians. They do not accept monopolizing the market. We have seen Microsoft being fined 561 million euros by the European Committee for not offering their users a browser choice in Windows 7. Apple has been fined 900.000 euros by the Italian competition authority for not complying with the 2-year compulsory warranty on their products.

We can conclude that cyber security has become an integral part of everyday life, an integral part of doing business. And that connectivity is a prerequisite for the normal functioning of the economy. The Dutch economy and society are not able to function without it anymore. And that part of this is the interconnectivity exceeds organizations borders and country borders. Cyber security must keep pace with this development. Information security must be an integral part of an organization: for consumers, businesses, utility organizations and the government itself, that should set the example. They all must become partners in building a cyber-secure world in the effort to ensure a stable and trusted environment. The developments within the economics of security mentioned above, show that Split Responsibility is not a viable option. An Alliance is a prerequisite for a secure economy.

Granted the cooperation is mostly advocated within a value chain and do not include the customer. But if an organization is responsible up to and including the border router we would not be putting enough liability on an organization in order for the economic incentive to work. An organization would not benefit from making a solution more secure because they do not suffer the consequences.

Jules Vandalon, vandalonja@gmail.com

The Joint Responsibility alternative would do justice to the interdependencies. The liability can be placed where it ought to be placed and a secure economy can be the result. The last alternative of Full responsibility also is a viable option from an economic point of view. The manufacturer has full responsibility and can be held liable if the solution leaves much to be desired. So the economic incentive is there. But organizations have to be careful not to monopolize the market by taking the Lock-in effect one step to far.

2.1.3. Socio-cultural dimension

Social-cultural factors include age distribution, population growth rate, employment levels, etc. Here the Socio-cultural factors of cyber security and information security are discussed in relation to customer and organization. The information below is from the Organization for Economic Co-operation and Development (OECD) (OECD Stats, 2015).

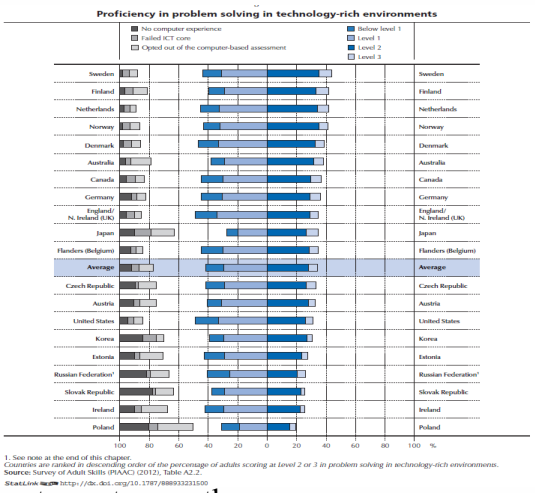
Money is an important means to achieving higher living standards that in turn is a prerequisite for buying devices, access to the internet and acquiring the skills that go with it. In the Netherlands, the average household net-adjusted disposable income per capita is 27.888 USD a year, more than the OECD average of 25.908 USD a year. But there is a considerable gap between the richest and poorest – the top 20% of the population earn more than four times as much as the bottom 20%.

Employment is another important factor in acquiring computer skills. In terms of employment, 74% of people aged 15 to 64 in the Netherlands have a paid job, above the OECD employment average of 65%. Some 79% of men are in paid work, compared to 70% of women.

The last element discussed here as a prerequisite for computer skills is education. Education and skills are important requisites for finding a job. In the Netherlands, 73% of adults aged 25-64 have completed upper secondary education; lower than the OECD average of 75%. In terms of the quality of the education system, the average student scored 519 in reading literacy, math, and science in the OECD's Program for International Student Assessment (PISA). This score is higher than the OECD average of 497, making the Netherlands one of the strongest OECD countries in students' skills.

We can conclude that the prerequisite needed for customers to have sufficient computer skills is present in the Netherlands. This is supported by the outcome of the OECD ranking of the Netherlands on the third place in their report about computer skills (OECD, 2015). The report reveals the extent today's adults can and do use computers to solve problems in their work and personal lives. The report shows that the ability to use computers is becoming an essential skill, and proficiency in computer use has an impact on the likelihood of participating in the labor force and on workers' wages. From these figures we can conclude that proficiency in computer use differs from customer to customer: there are different groups to be considered. If an organization wants to form an Alliance with the customer it has to decide to either create generic required measures on the lowest level required, in order to make sure that all customers are able to understand it. Or they should create different required measures per customer group (where groups are defined based on the customers' proficiency).

Figure 6 OECD ranking proficiency in computer use



1. See note at the end of this chapter.
Countries are ranked in descending order of the percentage of adults scoring at level 2 or 3 in problem solving in technology-rich environments.
Source: Survey of Adult Skills (PIAAC) (2012), Table A2.2.
StatLink http://dx.doi.org/10.1787/888933231500

Awareness of citizens/ consumers is also a prerequisite for cyber security. The Human Factor has extensively been researched. In his book Lacey describes it as "People are the soft underbelly of our information security. They design, implement and operate our information systems. They use misuse and abuse them. They manage the physical and logical access to our systems and data. In doing so, they create mistakes, incidents, and the weaknesses that enable criminals to steal, corrupt and manipulate our intellectual assets" (Lacey, 2015).

Schneier confirms that the human is the weakest link in his article 'Websites, passwords, and consumers". He also states: "It's one of the most important lessons of internet security: sometimes your biggest security problems are ones over which you have no control" (Schneier, Websites, passwords, and consumers, 2004). He is referring to the customers of American banks, having to make good on the customers' losses.

About the awareness of cyber security of Dutch consumers: According to governmental research (DutchGovernement, 2013), the awareness of cyber security amongst citizens has increased. However, despite this increase, the risk perception amongst ICT users is still limited and there is a large risk related to overconfidence. Dutch citizens rank their cyber security skills as a 7, this is, according to this research, overrated. For example, 66% of respondents didn't know how their device could be used for malicious activities and passwords most often do not comply with the advised security standards (DutchGovernement, 2013).

We can conclude that the Split responsibility alternative has some difficulties trying to uphold it. There is still a large part of the consumers' population that does not have the knowledge and skills to take responsibility. Granted an organization can choose, it does not have to do business with this part of the population. But excluding groups of consumers upfront seems poor business judgment. With the Joint responsibility model, we must take into consideration the different groups that were identified or we have to create an Alliance based on the lowest level of proficiency. There seems no barrier for the Full responsibility alternative. The organization takes care of everything and the consumer does not have to worry. As we have seen with the Apple cooperation it is possible to take care of almost everything and become one of the most secure solutions out there. Limiting the freedom of the consumers to a minimum and thanks to this / or nonetheless, be a commercial success. But there is one big issue with this alternative. The human is the weakest link. Not only the customer group with insufficient computer skills but also the other groups are susceptible to social engineering. Even good people make poor decisions. This is the biggest flaw in choosing the Full Responsibility model. An organization still has to address this issue. Or accept having to make good on the customers' losses.

2.1.4. Technological dimension

Technological factors include the rate of change, use of outsourcing, research & development, knowledge management systems, etc. Here the (Dutch) technological factors of cyber security and information security are discussed in relation to customers, organization, and the three alternatives.

The Netherlands finished in the fourth place (out of 147 countries) on the Networked Readiness Index (NRI) (INSEAD, 2015). The NRI measures the natural tendency for countries to exploit the opportunities offered by information and communications technology (ICT). It is a composite of three components: the environment for ICT offered by a given country or community, the readiness of the country's key stakeholders to use ICT and the usage of ICT among these stakeholders. We can conclude that the prerequisite of all the factors considered within the NRI are available in the Netherlands and thus all three models can be applied within the technological context. But not only should the foundation be available, also the technology to build and sustain solutions that can be applied, has to be available. From the organizations border router the Internet Service Provider, the device used with its OS and applications have to be secured. And technically that is possible. Also, techniques like Advanced Application Shielding have become mature. It essentially locks an application into a sandbox where it is not permitted to communicate with other applications. Many exploits tend to rely on operating systems' applications to launch an attack. If an application is locked down and prevented from communicating with other applications, you have essentially mitigated a big threat. (SANS 401). But all that technical power does not take the human out of the equation. The human remains the weakest link. Because the human factor already has been used within the socio-cultural analysis it is not used here. All three models are deemed feasible from a technical point of view.

1.1: The Networked Readiness Index 2015

Table 1: The Networked Readiness Index 2015

Rank	Country/Economy	Value	2014 rank (out of 148)	Income level*	Group†
1	Singapore	6.0	2	HI	ADV
2	Finland	6.0	1	HI-OECD	ADV
3	Sweden	5.8	3	HI-OECD	ADV
4	Netherlands	5.8	4	HI-OECD	ADV
5	Norway	5.8	5	HI-OECD	ADV
6	Switzerland	5.7	6	HI-OECD	ADV
7	United States	5.6	7	HI-OECD	ADV
8	United Kingdom	5.6	9	HI-OECD	ADV
9	Luxembourg	5.6	11	HI-OECD	ADV
10	Japan	5.6	16	HI-OECD	ADV
11	Canada	5.5	17	HI-OECD	ADV
12	Korea, Rep.	5.5	10	HI-OECD	ADV
13	Germany	5.5	12	HI-OECD	ADV
14	Hong Kong SAR	5.5	8	HI	ADV
15	Denmark	5.5	13	HI-OECD	ADV
16	Australia	5.5	18	HI-OECD	ADV
17	New Zealand	5.5	20	HI-OECD	ADV
18	Taiwan, China	5.5	14	HI	ADV
19	Iceland	5.4	19	HI-OECD	ADV
20	Austria	5.4	22	HI-OECD	ADV
21	Israel	5.4	15	HI-OECD	ADV
22	Estonia	5.3	21	HI-OECD	ADV
23	United Arab Emirates	5.3	24	HI	MENAP
24	Belgium	5.3	27	HI-OECD	ADV
25	Ireland	5.2	26	HI-OECD	ADV
26	France	5.2	25	HI-OECD	ADV
27	Qatar	5.1	23	HI	MENAP
28	Portugal	4.9	33	HI-OECD	ADV
29	Malta	4.9	28	HI	ADV
30	Bahrain	4.9	29	HI	MENAP

Figure 7 The Networked Readiness Index 2015

2.1.5. Legal dimension

Legal factors include taxation, employment, consumer, etc. Here the legal factors and Dutch laws of cyber security and information security are discussed in relation to customer and organization and the three alternatives. And responsibility, liability, and negligence are discussed in order to determine their impact on the three models.

An extensive study has been done by (Dommelen, 2013) on this subject in relation to Financial Service Providers in his paper '*Secure Online banking. A quest towards joint responsibilities'*. He constructed the model on page 6 of what element responsibility consists. He found the following.

The legal responsibilities of an organization are arranged in the Dutch Civil Code book 6 and 7. The first relevant element relates to the duty of care, arranged in article 6:248 BW (BW:6, 2013). This article relates to the generic duty of care of contracts and agreements. This article states that an agreement does not only have the - between the two parties agreed legal effects - but also those related to habits of reasonableness and fairness. Another connected article is article 7:401 BW (BW:7, 2013) which states that the contractor must, during the performance of work, take care of being a good contractor.

Dommelen argues that being responsible or acting in a negligent way in itself is not sufficient to be liable for something. He supports this by the theory of Bovens. Bovens described three generic categories that should be met in order to be liable: culpability, causal relationship and negligence (Bovens, 1990). Culpability means that somebody should be guilty of the offense of a standard. This means that there should be human behavior, an act or the omission that seems to have contributed to a situation. The standard refers to the standard of behavior that can reasonably be expected. Causal relationship means that there should be a causal relationship between the behavior and the act of a person and the resulting situation / damage. Somebody is liable when there is a causal relation between the act or the negligence of the person and the resulting situation. According to Bovens, it's not only important to determine if somebody - due to their actions - has contributed to the situation, the person should also be blameworthy for the act (negligent). This means that the person should have had real possibilities to act in a different way. All these three categories should be met in order to be liable. Dommelen further states that the Dutch civil law does not provide a generic answer to what gross negligence is. In her book about computer ethics, Johnson defines negligence as: "to be a failure to do something that a reasonable and prudent person would have done. In common law it is assumed that individuals who engage in certain activities owe a duty of care; negligence is a failure to fulfill that duty".

Thus, negligence presumes a standard of behavior that can reasonably be expected of an individual engaged in a particular activity (Johnson, 2001). In order to understand the situation, Dommelen first explored the more generic aspects of ethics in relation to a consumer / professional relationship by quoting Velasquez's work. Manuel G. Velasquez described three views about the relationship of business towards consumers. To him, it is clear that part of the responsibility for consumer's damages must rest on the consumer themselves since individuals are often careless in their use of products. The real question is where the consumer's duty to protect its interest ends, and where the businesses' duty to protect the consumers' interest begins (Valesquez, 1998).

Velasquez described three different theories in this regard: the contract view, the due care view and the social costs view "According to the contract view, the relationship between a business firm and its customers is essentially a contractual relationship, and the firm's moral duties to the customer are those created by this contractual relationship. When a consumer buys a product, this view holds that the consumer voluntarily enters into a 'sales contract' with the business firm. The act of entering into a contract is subject to several secondary moral constraints:

- both parties must have full knowledge of the nature of the agreement they are entering
- neither party of a contract must intentionally misrepresent the facts of the contractual situation of the other party
- neither party of a contract must be forced to enter the contract under duress or undue influence

Full knowledge implies that the seller has the duty to disclose exactly what the customer is buying and what the terms of the sale are. At a minimum, this means that the seller has a duty to inform the buyer of any facts about the product that would affect the customer's decision to purchase the product. For example, if a defect that poses a security risk exists, then the customer should be informed" (Valesquez, 1998). This view means that an organization has to explain all the defects, weaknesses and threats of their product to their customers.

With this Dommelen reaches the conclusion that the contract view is not applicable to the situation of cyber security since the customer doesn't have full knowledge of the nature of the product and its potential security flaws. An organization and customers do not share the same information and are not equally skilled in cyber security matter. Customers have to rely on the judgment of the organization.

"The due care theory of the business' duties to consumers is based on the idea, that consumers and sellers do not meet as equals and that the consumers' interest are particularly vulnerable to being harmed by the business who has a knowledge and an expertise that the consumer does not have. Because businesses are in a more advantage position, they have a duty to take special care to ensure that consumers' interests are not harmed by the products that they offer them. The business violates this duty and is negligent when there is a failure to exercise the care that a reasonable person could have foreseen would be necessary to prevent others from being harmed by the use of the product. A business is not morally negligent when others are harmed by a product and the harm was not one that the manufacturer could possibly have foreseen or prevented. Nor is the business morally negligent after having taken all reasonable steps to protect the customer and to ensure that the consumer is informed of any irremovable risks that might still attend the use of the product. For example, a business cannot be said to be negligent when the customer is acting careless or misusing the product. In determining the safeguard that should be built into a product, the business must also take into consideration the capacities of the persons who use the product. If the business anticipates that a product is used by persons that are too inexperienced to be aware of the dangers attendant on the use of the product, then the business owes them a greater degree of care than if the anticipated users were of ordinary intelligence and prudence.

The difficulty with this view is that there is no clear method for determining when one has exercised enough due care. There is not a hard and fast rule. A second difficulty is that it assumes that the business can discover the risk before the consumer buys and uses it" (Valesquez, 1998). Dommelen concludes that the second difficulty mentioned above can be eliminated when an organization has the possibility to inform their customer on newly discovered risks during the contract.

In order to do that, they need to know who their customers are and have the ability to communicate with them directly. The problem remaining for those organizations is to determine when enough due care has been executed.

"The social cost view holds that a business should pay the costs of any damages sustained through any defects in the products. Even when the business exercised all due care in the design and build of the product and has taken all reasonable precautions to warn customers of every foreseen danger. This theory is a very strong version of the doctrine of 'caveat vendor': let the seller take care. By having the business bear all the external costs that result from damages as well as the ordinary internal costs of design and build, all costs will be internalized and added on as part of the price of the product at the initial sales. Hence, informing the customer of the total costs of the sale. Second, since manufacturers have to pay the costs of damages, they will be motivated to exercise greater care and with that reduce the number of incidents. A criticism of this view is that passing the costs of damages on to all consumers (socializing the costs in the form of higher prices), consumers are also being treated unfairly. The second criticism of this theory attacks the assumption that passing the costs of all damages on the businesses will reduce the number of accidents. On the contrary, critics' claim, by relieving consumers of the responsibility of paying for their own injuries, the social costs theory will encourage carelessness in consumers. An increase in consumer carelessness will lead to an increase in consumer damages" (Valesquez, 1998).

Because of this increase, Dommelen concludes that the social cost view should not be followed. He concludes that because of the inequality in knowledge and positions between the customer and the organization and the fact that the customer doesn't have full knowledge, it is better to apply the due care view, instead of applying the contract view. He argues that the due care responsibility theory represents a joint responsibility between multiple stakeholders. The different stakeholders in the responsibility chain all carry different responsibilities. And together share the total responsibility, each in their own way. For example, the organization has the responsibility to secure their own platform and to inform their customers about the necessary and mandatory security measures. The customer has the responsibility to comply with these mandatory security measures.

Jules Vandalon, vandalonja@gmail.com

Another stakeholder with responsibility is the government, for example, by imposing new laws and regulations or improving the level of awareness of their citizens. He argues that based on the above statements it's difficult to defend that the customer has no responsibility at all. When being held responsible, it is important that all the elements of responsibility are present. Firstly, this means that the customers should know and understand their responsibilities. Communicating and understanding those responsibilities is a joint responsibility in itself. The organization should undertake sufficient efforts to help their customers to understand their responsibilities and to help them to take preventive actions. The customers and the society have the responsibility to take this matter seriously and to try to understand what is required. Secondly, this means that the customer needs to have the volition and ability to act according to these responsibilities. Customers should also understand the consequences of their actions, especially the consequences of not taking the required security measures. With his paper Dommelen comes to the conclusion that from a legal and responsibility point of view the best model to choose is due care responsibility theory.

The Split Responsibility model is difficult to implement from a legal point of view. It is difficult if not impossible to determine where the consumer's duty to protect its interest ends, and where the businesses' duty to protect the consumers' interest begins. And an organization and customers do not share the same information and are not equally skilled in cyber security matter. Customers have to rely on the judgment of the organization. The Joint Responsibility model comes close to the due care view and from a legal and responsivity standpoint is the best way to go as an organization.

The Full Responsibility model can be dismissed based on the risk that this would lead to an increase in consumer carelessness and with that an increase into what a consumer has to pay and other damages customers have to endure. An organization has to discount the losses due to damages into its prices. Therefore, this model is inferior to the due care model aka Joint Responsibility. But this is seen from an economic and social point of view. Not from a legal point of view as the law does not prohibit a Full Responsibility model. Because of this, the Full Responsibility is deemed possible to implement and maintain from a legal point of view.

2.1.6. Environmental dimension

Environmental factors include infrastructure, cyclical weather, disposal of materials, etc. Environmental factors of cyber security and information security could not be found in relation to customer and organization and the three alternatives. For all models, the score is neutral for the environmental dimension.

2.2. Advantages and disadvantages of the three categories

For each alternative, the outcome of the PESTLE analyzes has been summarized and put into the array to provide an overview of all that has been discussed.

Scoring: Positive = Green | Questionable = Yellow | Negative = Red | No color = Neutral

2.2.1. Split Responsibility

Responsibility / PESTLE dimension	Split	Joint	Full
Political dimension			
Economic dimension			
Socio-cultural dimension			
Technological dimension			
Legal dimension			
Environmental dimension			

From a Political point of view, this alternative is not acceptable. The European Union and the Dutch Government see an important role for organizations, securing customers. We can conclude that from the laws and rules and regulations that are in effect. Organizations are held liable if they do not comply with existing rules and regulations. From an economic standpoint, we would not be putting enough liability on an organization in order for the economic incentive to work for organizations to make secure solutions. As stated, security is not a problem of technology, but of misplaced economic incentives. From the Socio-cultural elements, we can also conclude that the Split responsibility alternative has some difficulties trying to uphold it. There is still a large part of the consumers' population that does not have the knowledge and skills to take responsibility. Communication and understanding the responsibilities is a joint responsibility in itself. And with that, we saw in paragraph 2.1 that lack of privacy and security were found to be significant obstacles to the adoption of, and a positive attitude towards a product.

An organization is not able to sell as much of its products as it would be able to sell with a product that is (perceived) as secure. Technically the Split Responsibility model is possible. From a legal point of view, the model has its downsides since the customer doesn't have full knowledge of the nature of the product and its potential security flaws. Therefore, the organization has the duty to inform and educate the customer. For all three models, the score is neutral for the environmental dimension. In the overview above we can see this model is the least able to create and sustain better information security and with that not able to create a better performance of the organization.

2.2.2. Joint Responsibility

From a Political point of view, this alternative is acceptable: both the organization and customer have to do their part. When they do, the Government will not step in and take (more) corrective action. From an Economical standpoint, the cost-benefit-ratio that holds companies back to make a better product is served best with this model. Businesses are intrinsically motivated to improve their product because it delivers the bigger turnover. Failing to do so will at best cost the organization customers and revenue; at worst put them out of business. With the Socio-cultural dimension, we see that it best tackles the weakest link in the security chain: The Human factor. By education, awareness training and taken into consideration the different groups, security, the organization, and the consumer are served best. Technically there are no obstacles for this model. From a legal point of view the Joint Responsibility model is seen as the best on two conditions; firstly, customers should know and understand their responsibilities. Secondly, the customer needs to have the volition and ability to act according to these responsibilities. For all three models, the score is neutral for the environmental dimension. In the overview above we can see this model is the best model to create and sustains a better information security and a better performance of the organization.

2.2.3. Full Responsibility

From a Political point of view this alternative is acceptable: As long as customers can do their business without risk or incidents and keep their faith in the products involved, and no monopoly is formed due to the Lock-in effect the model is acceptable.

The same goes for the economic dimension: as long as no monopoly is formed and the organization takes all responsibility there is no obstacle from this side. From the Socio-cultural point of view, the weakest link being the Human factor must be addressed. It is not possible to take the Human factor out of the equation, at least, no solution or evidence has been found that supports a feasible solution for this. Technically the model is possible, as for all three models. From a legal point of view, the Full Responsibility model can be implemented. Only economic factors stand in the way of implementing the model (hence the yellow score on economic dimension). It is based on the danger that this model would lead to an increase in consumer carelessness and with that an increase into what a consumer has to pay. An organization has to discount this loss into its prices. For all models, the score is neutral for the environmental dimension. In the overview above we can see this model comes second below Joint- and above Split Responsibility.

3. Conclusion

In the interest of security, continuity and sustainable performance of the organization the best way to go is Joint Responsibility. The organization and customer have a relationship. And in that relationship the organization has the better and stronger position. This may not be exploited. We see that through the political dimension; the customer is being protected. Organizations have to deal with this, or laws and regulations will. We see it in the economic factors were the liability should be placed in a way organizations are intrinsically motivated to make better secure products. Next to that more products are sold when they are perceived as secure. Another argument is the increasing dependence on connectivity for the normal functioning of society and economy. This forces an organization to take care of this in the best way they can: the multi-stakeholder approach and include the customer. The Human Factor in the Socio-Cultural dimension has to be addressed. Again by forming a relation with your customer and educating them, giving them tools and monitoring their behavior in order to protect them. And from a legal point of view, we see that responsibility has to be shared. This means that the customers should know and understand their responsibilities. Communicating and understanding those responsibilities is a joint responsibility on itself.

Jules Vandalon, vandalonja@gmail.com

4. Disclaimer

This paper is an exploration and is not advice, and should not be treated as such. Please keep in mind that the conclusions are based on the limited number of open sources. And are primarily based on the situation in the Netherlands, therefore, the outcome of this article cannot directly be applied to other countries. This paper can be seen as an initial investigation into this possible strategy. And can be the starting point for empirical research that substantiates the hypothesis. Or can be the starting point for your own PESTLE analysis for a Joint responsibility that applies to the country involved.

5. Bibliography

American Psychological Association. (2010). *APA Manual (Publication manual of the American Psychological Association (6th ed.).* Washington, DC: American Psychological Association.

Anderson, R. (2000). *Why Information Security is Hard - An Economic Perspective .* Cambridge: University of Cambridge Computer Laboratory.

Barnes, C. (2007). Initial trust and online buyer behaviour. *ndustrial Management & Data Systems*, Vol.107 Iss 1 pp 21-36.

Begum, N. J. (2008, February). The role of perceived usefulness, perceived ease of. *African Journal of Business Management Vol.2 (1)*, pp. 032-040.

Bovens, M. (1990). *Verantwoordelijkheid en organisatie.* Zwolle: W.E.J. Tjeen Willink.

Bratton, J. (2015). *Introduction to Work and Organizational Behaviour.* Palgrave Macmillan.

BW:6. (2013). *Burgelijk Wetboek 6 Verbintenissenrecht.*

BW:7. (2013). *Burgelijk Wetboek 7.*

CBS. (2015). *ICT, Kennis en economie.* Den Haag: Centraal Bureau voor de Statistiek.

Dommelen, P. v. (2013). *Secure online banking, a quest towards joint responsibilities.* Breukelen: Nyenrode Business University.

DutchGovernement. (2013, 10 28). *Nieuws*. Retrieved from Rijksoverheid: https://www.rijksoverheid.nl/actueel/nieuws/2013/10/28/alert-online-stimuleert-veilig-online-gedrag

European Commission. (2015, March 16). *Digital Agenda for Europe*. Retrieved from European Commission: http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive

Harrington, S. L. (2014, 12). CYBER SECURITY ACTIVE DEFENSE. *Richmond Journal of Law & Technology Volume XX, Issue 4*. Retrieved from http://jolt.richmond.edu/index.php/cyber security-active-defense-playing-with-fire-or-sound-risk-management/

INSEAD, W. E. (2015). *the Global Information Technology Report .* Geneva: World Economic Forum and INSEAD.

Johnson, D. (2001). *Computer Ethics.* Texas: Pearson Prentice Hall.

Jules Vandalon, vandalonja@gmail.com

Kuester, S. (2012). *MKT 301: Strategic Marketing & Marketing in Specific Industry Contexts.* Mannheim: University of Mannheim. Retrieved from https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDAQFjABahUKEwjnvvTHrPHIAhVJWxoKHcQxDWo&url=http%3A%2F%2Fwww.actuaries.org.uk%2Fsites%2Fall%2Ffiles%2Fdocuments%2Fpdf%2Fe01-understanding-comsumer-behaviour.pdf&usg=AFQjCNGuTftqwKxDfAKScT

Lacey, D. (2015). *Managing the Human Factor ininformation security.* West-Sussex: John Wiley &Amp; Sons.

Lee, R. M. (2015). *The Sliding Scale of Cyber Security.* Sans Analyst Whitepaper. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber security-36240

Morrison, M. (2013). *Strategic business diagnostic tools: theory and practice.* CreateSpace Independent Publishing.

NCSS 2. (2013). *National Cyber Security Strategy 2.* Den Haag: National Coordinator for Security and Counterterrorism.

OECD. (2015). *Adults, Computers and Problem Solving: What is the problem?* http://dx.doi.org/10.1787/9789264236844-en: OECD Publishing.

OECD Stats. (2015, 12 12). Retrieved from OECD: http://stats.oecd.org/Index.aspx?DataSetCode=BLI

Raaij, G. &. (1997). *Consumentengedrag.* Utrecht: Lemma BV.

Schneier, B. (2004, April 1). *Hacking the Business Climate for Network Security*. Retrieved from Schneier on Security: https://www.schneier.com/essays/archives/2004/04/hacking_the_business.html

Schneier, B. (2004, August 18). *Websites, passwords, and consumers*. Retrieved from Schneier on security: www.schneier.com

Schneier, B. (2006, June 29). *Economics and Information Security*. Retrieved from Schneier on Security: https://www.schneier.com/blog/archives/2006/06/economics_and_i_1.html

Schneier, B. (2008, Febuari 7). *Lock-in*. Retrieved from Wired.com.: Wired.com.

SecurityControls, C. C. (2015, October 15). *CIS Controls for Effective Cyber Defense Version 6.0*. Retrieved from SANS: http://www.cisecurity.org/critical-controls.cfm

Strunk, W. &. (1999). *The elements of style.* Boston: Allyn and Bacon.

Valesquez, M. (1998). *Business Ethics Concepts and Cases.* Prentice-Hall Inc.

WEF. (2012). *Partnering for Cyber, Risk and Responsibility in a Hyperconnected World - Principles and Guidelines.* Cologny/Geneva: World Economic Forum.