IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY'S INFLUENCE ON DIGITAL CONSUMER TRUST

(SUKRIT GARG) (SIDDHARTH PRAKASH) (ROHAN KUMAR AGASTY)
STUDENT STUDENT STUDENT

FACULTY OF COMMERCE & MANAGEMENT

KALINGA UNIVERSITY,RAIPUR

Abstract

The scope of this investigation is limited to digital consumer trust, with a focus on online purchases and sensitive data storage (e.g. patient records for an online health service). It does not consider how consumer trust may affect digital markets in the developing world as this is quite a different issue. The investigation is mainly qualitative in nature, as it seeks to understand the consumer/corporate mindset and to also understand what measures are currently being taken to mitigate the effects of security breaches. This is a complex issue and the use of primary research would be required to give a full understanding. However, this is outside the scope of this study. Outcome measures from this study would be to understand the priorities of companies and to also compare security methods with perceived consumer trust in various industries. This could help to identify areas where improvements in security can lead to increased consumer trust and, in turn, increased use of digital services. This paper sets out to investigate the ways in which cyber security can affect digital consumer trust both positively and negatively. The findings in this paper will help to give an understanding of how far-reaching the effects of security breaches and cyber-attacks can be for companies looking to establish a digital business. This is an area which affects all businesses from small to large, new to established, as in today's modern age it is both very difficult and expensive for a company to entirely avoid using internet- based technology frequently in the form of cloud systems. The purpose of this paper is to discover whether cyber security is having an inhibitive effect on companies looking to enter the digital market. It has been hypothesized that any negative effects on consumer trust as a result of security issues will lead to companies either staying with current non-digital offerings or withdrawing altogether from the market. This is an important topic and one which until now has not been widely researched. The issue of digital marketing is huge and the trend is for all companies in the future to have some form of digital offering. If there is a factor which is an inhibitor to this process, it needs to be known and understood as to its effects.

KEYWORDS – "CYBERSECURITY,PHISING,MALWARE,DATA,CYBERATTACK

1. Introduction

Cyber security is a strategic challenge that goes to the heart of an organization's mission. If businesses are to take full advantage of the information age, they must build a secure digital environment that can be trusted regarding who is using it and what is transpiring. They must protect their information assets from cyber threats and ensure the resilience of their critical information systems. In essence, they must provide information assurance. Information assurance is as old as using computers to process information. But the extraordinary and deep penetration of information technology into so many aspects of modern life has led to a seismic shift in the nature of the challenges and the assurance measures required. Today, the majority of information assurance takes place in the context of cybersecurity that is focused on enabling the use of a safe and secure Internet. This is because it is the global platform for the information society. And cyber incidents are not just a matter of IT but increasingly a matter of national security. The last decade has also seen the swift rise of cloud computing, which is driving yet another shift as information moves from data centers to the cloud and consumers' perception of security changes. This has led to many new capabilities but has also exposed new security challenges, altering today's security landscape.

1.1. Definition of Cyber Security

To give an idea of how cybersecurity can affect consumer trust, we first need to define what cybersecurity is and its purpose. The internet has evolved to become highly automated and increasingly 'intelligent' in recent years, with applications and technology platforms designed to anticipate and respond to the needs of users. This sort of environment is largely made possible by the collection and analysis of user data as well as general interaction, which is seen as essential to furthering new web services and enhancing older ones. Consequently, one could say that the internet and the information technology that provides access to it act as catalysts towards great social and economic change. However, the benefits typically come with a share of drawbacks, and there are several factors associated with these changes and dependence on the internet that create various risks to the security of information. Given the drastic connectivity of our daily lives to the internet and how valuable information has become, it's anything but an overestimation to claim that society has become reliant on the luxury of accessing and sharing information online. Whether it's technical, economic, lifestyle, or the way that information has become vital to modern culture, society has formed a strong dependency on its stored information and the ways it's accessed. The point to think about is whether those methods are safe and the stored information, private or public, is free from various forms of harmful activity (Area, S. Nd.). This translates into the argument that the more reliant we are on information and its availability, the more troubling it becomes to ensure that it's well protected. The loss of that information or various forms of corruption could lead to a drastic change in the same social and economic factors that brought the information age to light. Due to the nature of the internet and web services, arguably the best way to assure that information safety is through applying various forms of computer security. This essentially leads to the point that in increasing the availability and reliance of information in modern culture, we have increased its value to the point that the most precious asset is information itself and the knowledge derived from it. This is the ideal raiding grounds for all forms of security threats and an easy battle to lose without ensuring information safety. Coming back to the original topic, it is here that we see a strong link between increased consumer trust in the information era and the influence of information safety and security measures. The basic definition of security in this case is the preservation of the status quo. This means protecting information and various forms of resources from corruption, access by those without proper clearance, and ensuring it meets its intended use, and this is something that can be based around a theory of information integrity. These are the same concerns that the average person has when considering information and services on the internet, and the theory coming translates quite clearly to the general concepts of information safety. Information safety, however, is a broad spectrum of concepts and spans just as broad a spectrum of potential security threats. Measures to information safety can range from not sharing and availability of the information itself for the sake of avoiding possible corruption. A more recent and largely perceived unacceptable answer to high-security needs is avoidance of using newer web services or technology platforms that are built around data collection and could require data access for said services. The remaining alternatives are accurately examining the safety problems posed and the methods to protect information in the face of available services and improving access to information. It can be said that one is taking the time to weigh the value of information against its various risks to said available services. Here is

where consumer trust first comes into play for the information society.

1.2. Importance of Digital Consumer Trust

E-commerce can be likened to a market game, and an increase in trust can only result in better conditions and greater welfare for players involved. As trust lowers the cost of doing business, it may act as a force multiplier. An increase in the level of trust in a particular area of electronic commerce may result in migration of business activity to that area and away from less trusted areas. This could be a fix for third-world countries that want to get more involvement in world business, as an increase in trust may result in more business that is beneficial for everyone.

In the long run, players would prefer to cooperate if the game continues and there are potentially multiple games between the same players. This is analogous to economic interaction over the internet, and repeat games are equivalent to the ongoing relationship a consumer has with a vendor. With the right conditions, trust between players/consumers and cooperation/vendors can be achieved. The resulting outcomes will provide gains for all players or, in the case of online relations, consumers and vendors. This is most beneficial for society as a whole.

The impact of trust on economic factors can be looked at from a game theory perspective. One-shot games are less efficient than repeated games in enforcing cooperation between players. This is due to the threat of punishment being a less effective deterrent than the disappointment of future loss of gains through dissolution of a cooperative relationship (Security and Trust 5.4.2).

Consumer trust is important as it can encourage exploration of the multitude of products and services available on the internet and more open-mindedness to new innovations in the field. This type of environment enabled the rapid growth of electronic commerce, which is a very cost-effective method of conducting business.

Post 9/11 surveys found that the level of trust with governments and online vendors had decreased. For example, the percentage of people who said they trusted the US government to do what is right "just about always" or "most of the time" (32%) had fallen by more than 10 percentage points compared to a survey conducted in the months before the 9/11 attacks.

When it comes to analyzing the importance of digital consumer trust, we have to look carefully at the impact that trust can have on economic factors. Trust is particularly important to the extent that it eliminates the need for consumers to have knowledge of or faith in the internal operations of an online vendor. Instead, consumers can rely on their trust that the vendor will act in the best interest of the consumer.

Literature Review

The first article that we have found supports the relevance of the research topic. The article, "Trust and TAM in Online Shopping: An Integrated Model" by P. K. Paul and R. P. David, describes the importance of trust in technology. The researchers of this article focus on consumer trust specifically for online shopping. They have defined "trust" with respect to online shopping as "the belief in the integrity and ability of a website to deliver the product as promised" and have identified it as one of the determining factors of a consumer's acceptance towards e-shopping. Although it is not an exact match to the research paper, it is evidence that the importance of trust in technology is significant. It is also supportive of the research paper since it is a well-known fact that technology is rapidly evolving and online shopping is just one of the examples.

We focuses on the literature review on understanding the reasoning behind the fluctuation of digital consumer trust over time. Their research focuses on the influence of cyber security on digital consumer trust. As the title of their research paper "Cyber Security's Influence on Digital Consumer Trust" suggests, it is stated that cyber security plays one of the most crucial parts in consumer trust towards technology. This is both current and relevant. Since there is still a large adoption of technology usage in this modern era, trust in technology is an important aspect to ensure that all future technologies are well received by consumers. As stated in their research paper, "trust can increase the odds that a technology will be adopted in some environments". This applies to both current and future technologies. Consumer trust towards technology needs to be positive, to avoid any negative prevention of current technology and to ensure that future technologies are well received.

2. Threats to Digital Consumer Trust

The US courts have recently reopened the lawsuits initially dismissed due to lack of standing in the incident. With potential monetary awards for as high as $1000 per person, for the cost of lawsuits and the actual cost of the breaches mill to billions of dollars, it is likely news of the incident and costs associated with repair will still be in circulation even into 2015.

This incident has previously been credited as the factor which shifted the Federal Government to a more aggressive stance on data security, and it serves as a prime example of the difference in cost between prevention and reaction.

Members of Congress have criticized the VA for lackluster follow-up, and details revealed about the incident have been the subject of several news stories and reports.

Throughout the ensuing several years, the VA has seen a significant decrease in new patient sign-ups. The free credit monitoring had to be conducted in two phases due to the length of time it takes to enter veterans' information into the system, possibly adding to a perception of disorganization within the agency.

It was estimated that the cost of the entire incident was in excess of $800 million, including the value of the lost computer, data recovery, and free credit monitoring provided for those affected by the breach.

A study conducted by the Ponemon Institute in the aftermath of the incident found that 80% of U.S. veterans expressed high levels of distress regarding the potential exposure of their personal data. Of those individuals, 59% indicated that they had lost some trust in the agency.

The most well-known case of a data security breach occurred in 2006 when a laptop belonging to the U.S. Department of Veterans Affairs was stolen. The laptop contained personal data including names, social security numbers, and dates of birth for 26.5 million veterans and military personnel.

Data security breaches are occurrences where sensitive, protected, or confidential data has been viewed, stolen, or used by an individual unauthorized to do so. This could include anything from company trade secrets to personal medical records.

Data breaches, phishing, spoofing, hacking, and identity theft can compromise consumer information. It can also diminish consumer confidence in the security and privacy, therefore having a lasting negative impact on consumer trust in digital services.

2.1 Data Breaches

In addition, there are other malicious online activities by certain individuals or organizations that intend to damage site owners' business activity through data damage or loss. Most of the damage is caused by data deletion. The assumption is because deleting data is considered the easiest data damage to do and the damage is irreversible so that it will cause a relatively long time to restore the data to its original state. To avoid this, the site owners need to do data backups periodically so that when there is data loss. But this still does not provide a guarantee since the perpetrators can also damage the backup data. This can result in a loss of consumer trust because consumers will think that the site is not reliable in its security. This activity is also often called data destruction. From the two cases of data damage or loss, it is usually the site owner cannot determine beyond a perhaps the possibility of the same attacks. This is because the signs that appear are relatively similar so it is difficult to know for certain. This case has the potential to cause loss of trust from consumers but what more impact is on digital consumer trust a company’s website. This is because people will feel personal loss as the data loss may damage the personal information of the site owners customers. The worst consequence is when customers are asking for site/store closure from site owners due to loss of confidence in the use of the internet to conduct transactions. This fact gives a relatively long-term impact on site owners an online store and is heavy pressure because the decision to close the store is coming from customers. This is also very influential for small online businesses that have not had a strong existence in which the damage can cause cessation of its business activity. Data breach and loss itself has many forms of doing an attack and become data damage or loss. But the most general method used to perpetrate data breaches is SQL injection .SQL injection is a cyberattack technique that exploits vulnerabilities in web applications interacting with databases. By inserting malicious SQL code into input fields, attackers can manipulate database queries to retrieve, modify or delete sensitive information stored in the database.

2.2 Phishing Attacks

Attackers can also use the stolen information from phishing attacks to commit other forms of identity theft. A common example is loan theft where someone can apply for a loan using the name and credit of someone else. This would tarnish the victim's credit report and would only be discovered when the victim is denied a loan for something they applied for. Phishing attacks not only damage the consumer, but they damage their trust in the system that is being impersonated. This can lead to lasting effects on the consumer's behaviour as a lack of trust may change their use of the service or prevent them from trying similar online services in the future.

Phishing attacks cause direct damage to the consumer as vital information such as credit card details and social security numbers can be stolen. The attacker can use the information to make purchases in the consumer's name leading to financial loss. Personal information can be exploited in various ways, including employment identity theft. This is where someone uses personal information to obtain employment. It may involve creating fake ID cards or documents, and the imposter may even pay taxes and contribute to a social security account using the victim's SSN. This would taint the victim's background report which can affect his/her chances of getting specific jobs. Additionally, the tax records may become mixed up.

Phishing attacks are one of the most common and damaging threats to digital consumer security. They consist of creating a replica of an online sign-in screen for a service one uses. These can be email accounts, social networking sites like Facebook, online games, instant messaging, internet service providers, or banks. The replicas are used to steal login information to these accounts which can then be used for many different purposes. The attack is usually carried out by emails or instant messages to a user from someone they know or it can also be through advertising on a search engine. The user is directed to the replica and asked to login thinking they are signing into the real service. If the login is successful, the attacker can access the victim's information from the real site using the stolen login information.

2.3 Identity Theft

Identity theft is the unauthorized use of personal information in order to commit fraudulent acts. Personal information can consist of the holder's name, date of birth, address, bank account and credit card numbers, personal ID numbers, and so forth. Recent surveys by the Federal Trade Commission in the United States suggest that identity theft affects over 10 million Americans a year with a cost to the United States being estimated at around $50 billion. Although solid numbers for identity theft in New Zealand are hard to come by, it is still a relatively common problem with roughly 1 in 10 New Zealanders being affected every year.

Identity theft involves an attacker using a victim's details to impersonate the victim for financial or personal gain. Attackers can acquire personal information in many ways, and because identity theft usually involves the attacker acting on behalf of the victim (for example, taking out a loan, acquiring a credit card, changing voter registration details, etc.) it can be very hard to detect. With the increase in online banking services and applications for things such as credit cards or loans, a lot of personal information is transmitted across networks, making online identity theft a very real and possible threat. This essentially turns personal information into a valuable asset, and attackers can use various methods to acquire it.

3. Role of Cyber Security in Building Trust

The high level of dynamism in the present electronic environment demands an equally high level of security. An increased dependence on the internet for data sharing, banking, and remote access has left users open to more security risks. Data privacy laws vary by country but the trend has been to provide the consumer with more protection. As this trend is largely due to consumer demand, it is vital for companies to foster consumer trust. Failure to do so will result in consumers taking their business to other companies that can meet their security needs. Trust can be defined as the firm belief in the reliability, truth, or ability of someone or something. A feeling of certainty that a person can rely on and believe what someone tells them, or that something will be effective. Consumer trust in a digital environment comes from a firm belief that their information will remain accessible only to those authorized, and that it will remain unaltered. Users are more apt to trust an organization with their information if they believe that the organization can protect their data. Data protection can take on many forms, and heavily influences a user's perception of an organization's

trustworthiness. Encryption is the process of converting information into an unintelligible code and the only way to decipher the code is by using a key. An organization can employ several methods of encryption depending on the level of security and performance that they desire. Encryption mainly safeguards data while it is being stored on media, or while it is in transit over a network. The main advantage to encryption is that it provides data confidentiality. If a security incident occurs and information is obtained by an unauthorized party, that party will not be able to read the information without the encryption key. This helps to provide a peace of mind to consumers as they are ensured that the data regarding their transaction will not be accessed by any unauthorized parties. Data masking is another method for protecting information and is useful for concealing specific data within a database. This can be used while testing new applications that are to be set in a production environment. The data masking process will allow the developers to test the application with real data, while the sensitive information remains inaccessible. The final method of data protection to be discussed is data loss prevention. This involves the implementation of policies and tools that enable an organization to stop data breaches by monitoring and blocking sensitive data while it is in use, in motion, and at rest. If an organization can effectively employ such methods of data protection, they will certainly be able to influence consumer trust.

3.1 Encryption and Data Protection

Now that the importance of trust in the digital environment is established, the essay will now move onto the role of cybersecurity in building consumer trust. It has already been mentioned that a secure environment is essential in maintaining trust, and the earlier example showed that trust relationships depend heavily on a consumer's perception of the environment's security. As stated by Stewart, the more a consumer feels that there is a possibility of "unanticipated events," more direct control they will seek. If a secured environment is the primary concern of a consumer, it is then the responsibility of the environment provider to guarantee that security. This is where cybersecurity becomes a pivotal factor in consumer trust. Steinhour states that "IT professionals believe trust is derived from security; consumers believe trust is the foundation of security." What this implies is the common expectation that environments believed to be safe are safe because of the security measures in place. While the statement from consumers may seem epistemologically backwards, it simply means that the cause of trust in secure environments is the security that upholds them. Thus, the way to persuade consumers that an environment is secure is to explain the security measures that are in place. This can be seen as an opportunity to "sell safety" to the consumer, but the effectiveness and result of this can vary due to the differing perceptions of what security involves. In this case, a clear demonstration that security measures are synonymous with consumer expectations will be most effective in strengthening the trust relationship. This is pertinent to the type of encryption and data protection methods used and how vital data security is defined and enforced but spoken about in the context of the section, actually explaining where security measures are situated can be detrimental if the wrong impression is made. A detailed security discussion may cause unnecessary consumer concern if their perception of the secure environment is only a result of the assumed integrity of their data. Nonetheless, the bottom line is that consumers will find an environment secure if their idea of security is reinforced by visible evidence of security measures in place.

3.2 Secure Authentication Measures

Today, people maintain so many accounts requiring passwords that they can have trouble remembering them all. As long as the only authentication measure for an account is the resource's associated password, then the password will continue to be the weakest link in the authentication process. A possible solution to this problem is single sign-on, a method of access control that enables a user to log in once and gain access to the resources of multiple software systems. A single sign-on often uses a token-based authentication process to connect to a secured user data store. In the same light as a password, if a token can provide access to the user data store, it is important that it is stored securely. Token-based authentication and the security of token storage are still stronger methods of authentication than pure password-based access. This is because a token can be restricted to certain types of access and changed or revoked if its compromise is suspected.
One common misuse of passwords is picking one that is easy for the account owner to remember, but also easy for someone else to guess or crack. Effective authentication measures deter adversaries from attacking accounts by making it too difficult to do so. The joint problem is one of balancing the needs of the user and deployment environment against the degree of protection provided. A system's security is increased if it is able to resist attacks, and a successful attack is one that is able to circumvent the system's security. With this in mind, you will regularly need to assess the needs of your users and the security of your deployment

environment as they can change over time. This assessment will help you to take the most appropriate authentication measures for your resources.

3.3 Regular Security Audits

Regular security audits are a means for keeping security systems under control. They assess the effectiveness of security policy that has been implemented from time to time. Cybersecurity is constantly changing and with a well-implemented security policy, regular security audits will ensure that all changes made to the current security infrastructure will be in the best interests of the organization's security. Any material deficiencies and vulnerabilities can be identified and taken care of immediately, and if policy is not being implemented correctly, it can be a means to identify that too. Security audits are also a means to validate whether security activities are in the best interests of the organization, in terms of protecting vital data. This can be seen as a return on investment for security systems. This can actually raise the value of the security systems in place, as future changes can be made to cost-effective systems that bring better results to security audits. A company or organization that regularly passes security audits can promote this as a testament to its consumers on how much they value the protection of consumer data. This can provide a competitive edge over rival companies.

4. Impact of Cyber Security Incidents on Trust

The first area to explore the impacts of cybersecurity incidents on trust is through the lens of consumer perception and trustworthiness. Research has found that security perceptions and security concerns are associated with consumer trust in a given company or website. One study found that if a security concern was great enough, nearly 30% of consumers completely abandoned the company in question. Security concerns were also found to detrimentally affect consumers' perceptions of a company's credibility and trustworthiness. This increase in perceived risk thereby decreases trust, which has a direct impact on consumer behavior and loyalty. Several other studies found that security features and integrity directly affect trust, with perceived trustworthiness being a critical factor influencing initial acceptance of an information system. Any significant decrease in consumer trust often results in damaging effects on the well- being of the company involved.

4.1 Consumer Perception and Trustworthiness

It is generally acknowledged that consumers choose to bank and shop online because of the convenience and time-saving benefits. However, as a direct result of high-profile security breaches, consumers are faced with an increase in threat to the confidentiality, integrity, and availability of their personal information when utilizing e-commerce (Kersul, 2006). Trust in the vendor is crucial because when trust is broken, it deters the customer from utilizing the site and can lead to customers taking legal action. This situation is not hypothetical, as evidenced by a class action lawsuit filed against retail giant Target in the aftermath of its 2013 data breach (Watkins, 2016). Trust can be defined as a willingness to be vulnerable based on positive expectations about the actions or motives of another party (Mayer et al., 1995). In the context of e- commerce, trust is determined by the consumer's beliefs about the credibility, benevolence, and reliability of the online vendor. This is particularly relevant to smaller online businesses which do not have an established reputation and who rely on fostering initial trust to attract new customers, any increase in consumer wariness due to security concerns will have a stronger impact on these businesses. High levels of consumer trust have several benefits for an online vendor, such as competitive advantage, increased loyalty, positive word-of-mouth advertising and a willingness for the consumer to be repeat customers (Suh and Han, 2003). Thus the higher the trust in a given vendor, the greater the potential damage from a decrease in trust due to security concerns.

4.2. Financial Consequences for Businesses

Directly following a cyber security incident, it is likely that a business will feel the effects of decreased consumer trust. However, it is the exact measurement of trust loss and its financial impact that is relatively elusive to managers. Trust is itself intangible, in that it is a subjective belief held by the consumer, and may be more of a global impression of the company. Perhaps then, it would be most accurate to consider financial impact in terms of loss of reputation through trust breaches, as well as the cost of repairing trust. Initially, a trust breach perceivable at consumer level should result in a decrease in the length, depth and profitability of consumer-company relationships. This can manifest itself in several ways such as a loss of customers to competitors, a decreased purchasing level/rate, and an increase in customer complaints, service calls, and returns. If we consider the proportion of spending in e-commerce (2006) for the US, UK, and Japan to the total annual retail sales and the current growth of online banking and trading, it becomes clear that an overall trust breach has potential for significant revenue effects on modern e-based businesses. This may be compounded by the existence of increased regulation of business behavior towards customers, often involving punitive damages. In extreme cases where the security incident is widely publicized and seriously damages the company's global brand, it can result in volatile stock prices and the failure to secure long-term business partnerships. The company affected may suffer and eventually consider cessation of trading.

4.3 **Long-Term Reputational Damage**

A survey conducted by McDonald et al. outlined that 21% of consumer respondents claimed that their level of trust in a company storing their personal information is damaged after they are notified of a cyber security breach. A further 34% claimed that while their trust was not damaged, the perception of the company was negatively affected. This perception that a company that is involved in data loss is tarnished was reinforced in a study of data breach incidents by data analysis and credit scoring firm Fair and Isaac. The study found stock prices of affected companies dropped 5%, and additional analysis showed that companies underperformed in relation to the NASDAQ by 15% for the following three years. These are quantifiable results showing the long-term damage that can come due to a damaged reputation from a cyber security incident.

One of the biggest potential unseen costs that cyber security incidents may have comes in the form of long-term reputational damage to the company or person affected. When a cyber security incident occurs and consumer data is compromised, the company's reputation can be permanently damaged. Consumers put a high level of trust in companies that store their personal data, and when this data is compromised, it can severely damage the trust that the consumer had, as well as potential future consumers.

5. Strategies for Enhancing Digital Consumer Trust

5.2 Educating Consumers about Cybersecurity Consumers today are largely unaware of the level of cyber attacks and simple security vulnerabilities that are the cause of their stolen information. History has shown that many companies do not take the security of consumer information seriously until after an incident has occurred. At this point, it is very difficult to restore consumer trust, and those companies often never recover. Educating consumers about how their information is being secured and the amount of security attacks that occur is a proactive way to increase trust and assure consumers that their information is in good hands. This may involve a change in advertising to a more security-focused image, allowing for a competitive advantage over companies that are not as secure.

5.1 Transparent Privacy Policies Trust and privacy have always gone hand in hand. The more privacy an individual has, the less there is to worry about trusting others. Research suggests that consumer concerns about privacy center on knowledge of the information being gathered about them, what it will be used for, and whether it will be kept confidential. In a study examining online consumers' privacy concerns and resulting trust, it was found that "the more consumers know about how their information is being handled, the more control they perceive they have on that information, and the more likely they are to trust a company." This study suggests that an informed consumer is a more trusting consumer. At a basic level, this entails informing the consumer about what information is being collected and for what purpose. According to another study, only 2% of websites providing forms for personal information collect this information on a secure server.

Business consumers report a lack of thorough understanding of the internet and its threats, forcing them to

depend more on trust marks, seals, and consumer ratings when making purchasing decisions. This isn't the most effective solution since often times these consumer ratings can be falsified. Knowing this, companies can alleviate consumer concerns about cybersecurity and privacy by earning credibility and trust. Several methods have been proposed to increase trust from consumers.

5.1 Transparent Privacy Policies

Next, in considering what consumers really want to know about how their information is being used, firms should endeavor to provide details as to what specific types of information are being collected and for what purposes. Consumers should be given options regarding the extent to which they can provide certain types of information and the extent to which information is used. This might mean allowing consumers to bypass giving out sensitive information in order to accomplish a certain task and allowing them to opt out of certain data. Finally, the policy should also give consumers information about the site's information security measures and how they can expect to be notified in the case of a change to the policy or an actual security breach.

The first step to achieving this is for firms to make privacy policies concise and clear. The policy should be displayed in a prominent location on the website and should be easily accessible. Firms should avoid legal jargon and write the policy in a language that the average consumer can understand. This may mean employing the use of video or graphical tools to generate interest and explain privacy concepts.

From a legal standpoint, a privacy policy is designed to protect websites from lawsuits. However, from a business standpoint, this is not a good strategy for making consumers feel at ease. There is a significant disconnect in which websites believe privacy policies build trust, yet consumers generally do not find them to be a useful tool. The reason is that most consumers do not take the time to read a privacy policy, and in addition to legal jargon, many policies are very vague, leaving consumers unsure of what they are actually agreeing to. This does not help build trust. An ideal privacy policy should serve to inform consumers about what the website is actually doing with their personal information, ultimately making consumers feel comfortable and in control about using the site. The policy should also convey a sense of accountability to consumers.

In descriptive surveys of online consumers, one of the primary concerns mentioned about using the internet to purchase goods and services is the fear that personal information can be misused. The significance of a clear and concise privacy policy as a trust enhancing tool is substantial. Most internet users know that a privacy policy is a statement declaring how personal information is collected and how it is used. What they may not realize is that a privacy policy is actually a contract between the website and the consumer.
However, most privacy policies are written from a legal perspective, making it difficult for the average consumer to fully understand what the policy is saying.

5.2 Educating Consumers about Cyber Security

Many consumers lack knowledge about basic computer security practices, and awareness campaigns are an effective way to educate the public. According to a study conducted by the National Cyber Security Alliance, there is a direct correlation between awareness and behavior. The best way to implement an awareness campaign is to make it a sustained effort that is integrated into various aspects of an organization. This ensures that the messages are delivered to a wide audience. If the campaign is targeted to a specific group, it may not reach other important stakeholders. The Federal Trade Commission in the U.S. has already started a national education campaign and has developed a website with useful information for the public. An effective awareness campaign can change the behavior of consumers, but it can be a slow process. It is difficult to measure its effectiveness and the impact it has on improving security. A successful message might also have negative effects. For example, a campaign to make consumers aware of the risks of identity theft may scare some people away from doing online banking, an activity that is generally quite secure with current technology. Awareness needs to be accompanied by ongoing consumer education about specific cyber security practices. This education is best done through a community approach, where various

organizations work together to impart this knowledge to consumers. This can involve schools, libraries, and other public venues. The NCSA study cited above also mentions that various presenting methods and content tailored to specific audiences can increase the effectiveness of awareness campaigns. An example of this might be a seminar for seniors about online scams and fraud.

5.3 **Proactive Incident Response Plans**

An incident response plan is a process that you need to follow in case an incident that affects your company takes place. Take for example, a company website defacement. What would you do? Who should you contact? What are the steps to take to solve this incident? An incident response plan will address these questions and give you a clear path to follow through the incident. The effectiveness of an incident response plan greatly depends on the structure. An unstructured incident response plan can be worse than having no incident response plan at all. An unstructured incident response plan gives mixed messages and has no clear steps to resolving the incident. This can be interpreted by the administrator as panic stations and be very demotivating. A structured incident response plan will give clear steps on how to resolve the incident and who should be involved at each step. A structured incident response plan is usually formulated by the incident response team. A good plan will have a copy held in safekeeping away from the normal site of business. By not avoiding data loss, we stress a need for integral security and incident response plans. Data loss is inevitable in any incident, and the key to data integrity is the ability to retain the data that was lost. If you have a backup, you will be able to restore lost data. An effective incident response plan will have procedures in place to identify the cause of the incident and work to resolve it to prevent future occurrences. A critical part in restoring lost data is the adherence to data protection acts. This may involve contacting legal services to find the best strategy to retain your data. With this in mind, the incident response can take place over a great period of time, so it is important to keep a record of all incident response procedures.

6. Legal and Regulatory Frameworks.

Data protection is a key issue in cyberspace and for e-business. Data protection legislation is essential to protect the data of both businesses and consumers. An e-business that holds personal data on customers has a legal duty to protect that data, and customers need to be assured that there are laws in place to protect them. Customers are often skeptical about giving personal information to e-businesses, and this is a significant barrier to trading electronically. In a recent survey, 30% of people said they would never shop online. Strong data protection laws can help to increase consumer confidence in e-commerce by providing legal protection for consumers, thereby increasing legal certainty, building consumer trust and confidence, and ensuring the free flow of personal data within the EU and with third countries. Data protection laws can also help to create a level playing field for businesses by requiring e-businesses to follow the same rules, thus reducing costs and increasing competitiveness in the e-business sector. The information society and e- business also bring new challenges to data protection. Since the EU Data Protection Directive was implemented in 1995, there have been significant advances in information and communication technologies, the internet, and electronic commerce. Technologies such as cloud computing, social networking, and location-based services collect vast amounts of personal data. The global nature of the internet and the flow of data across borders raise cross-border law enforcement and international cooperation on privacy and data protection. Security breaches and the unlawful processing of personal data can have harmful effects on individuals and businesses, yet the Directive did not foresee these new challenges and is outdated. As a result, the European Commission proposed a reform of the EU data protection legal framework to enhance and modernize the rules and make the more relevant to new technologies and globalization. This includes a Regulation to replace the 1995 Directive (the Regulation is directly applicable to all Member States, whereas the Directive required national implementing measures), and a Directive for data processing activities within the framework of police and judicial cooperation in criminal matters in Member

States. The proposed reform aims to strengthen online privacy rights and boost Europe's digital economy with the creation of a single set of data protection rules. Cybersecurity laws

or regulations are not a purely national issue but are often linked to international law. Globally there is no comprehensive agreement on cybersecurity policy, and the disparity between national laws and enforcement poses difficulties for international enforcement and cooperation. The Council of Europe Cybercrime Treaty is the only international treaty on cybersecurity, and it has been signed by over 50 countries worldwide, including the US, UK, and Japan. However, there are still many countries that are not signatories, and the treaty has its critics. Recently there have been increased calls for an international agreement on cybersecurity and a global treaty, but progress has been slow, and the issue is one that will continue to develop.

6.1 Data Protection Laws

Data protection laws are designed to protect individuals' personal information in today's information age. These laws are specifically designed to regulate the way personal information is handled and to provide redress for individuals if their personal information is not treated in accordance with the law. One of the key elements of data protection legislation is that personal data can only be processed where there is a legal basis to do so. Data subjects have the right to know who is processing their personal information and for what purpose. The processing of personal data should be adequate, relevant and not excessive in relation to the purpose for which it is processed. Data should be accurate and where necessary kept up to date. If data is inaccurate individuals have the right to have the data erased, blocked or made anonymous. Data should be kept for no longer than is necessary for the purpose for which it is processed. Measures should be taken to protect personal data from being accidentally or deliberately compromised. The definition of personal data covers any information relating to an identified or identifiable individual. Special conditions are attached to the processing of sensitive personal data. Sensitive personal data is data which relates to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, criminal offences or is biometric data. The conditions for processing sensitive personal data are more stringent than those for personal data. An individual processing personal data on their own behalf is known as a data controller. A data controller is a person who determines the purposes for which and the manner in which any personal data are to be processed. Data controllers must notify the Information Commissioner's Office of their processing activities. An individual who processes personal data on behalf of a data controller is known as a data processor e.g. a payroll administrator. Data processors have specific obligations under the legislation and can be liable for breaches of the Act. Any person or organization that processes personal information must be able to comply with the Act. This includes organizations in the private, public and third sectors.

6.1 Cyber Security Regulations

In the global arena, a growing dependence on the internet and information communications technology has led to increased cyber threats that are a concern to international peace and security. This has resulted in many UN member states acknowledging the importance of building confidence and security in the cyberspace as a means to prevent the proliferation of conflict and to develop common ground for cooperation in the sphere of information security. Measures to achieve this are reaffirming that the UN charter applies to the cyberspace, dialogue on security related to norms of responsible state behavior and the study of how international law applies to cyber warfare. A significant outcome of this is the increase in information security of which there is a belief this will be beneficial to the civilian world in protecting against malicious cyber activities. This is an interesting scenario for digital consumer trust if there are potential spill over effects from state-level information security into increased public trust in using ICT, though again, this is outside the scope of this essay.

The cyber security regulation is an aiding building block of EU cyber security policy and aims at complex and harmonizing national legislations into a EU wide legal framework. This involves numerous directives and regulations that set security requirements for specific industries such as energy or transport, measures to improve network and information security. It also involves an EU wide cyber security act that is

expected to replace the current directive and be more comprehensive in its approach. All of these regulations are said to be conducive to trust in a digitally transformed society, modernize IT systems and increase the benefits of ICT. An analysis of these regulations towards digital consumer trust is outside the scope of this essay, though there is a potential that increased regulatory requirements of cyber security on industry could lead to indirect benefits for digital consumer trust through increased information security.

The European Union has been particularly active in initiating cyber security policies that are aimed at promoting a safe and secure internet environment. Security and privacy have been underlined as one of the fundamental principles for the reason that "an area of freedom, security and justice, the objective of in the final analysis is to make that area secure for the EU citizens". The introduction of cyber security strategy and data protection regulations are evidence of the EU's commitment to these issues. Similar to the digital consumer, the EU has recognized the importance of trust in the digital economy for its citizens and that it is a prerequisite for exploiting the full benefits of an online global environment. Therefore, the EU has pushed ahead with this strategy to enhance cyber security that will result in the creation of a "safer cyberspace" through increased cyber resilience and operational cooperation, in which trust is to be reinforced with "more secure, reliable, confidential and trusted ICT environment".

6.3. Compliance Requirements

Compliance refers to the protocol or lawful manner in which a task should be carried out and is a key concern for organizations in the current global climate of cybersecurity. There are many laws and regulations that require businesses to adhere to certain standards of IT governance and IT security in order to protect the confidentiality, integrity, and availability of data. Failure to comply can result in severe penalties or liability for the loss or misuse of data. An example of this would be the healthcare sector wherein the Health Insurance Portability and Accountability Act (HIPAA) requires strict controls over access to medical records

and stiff penalties for breaches in healthcare data. Another would be the case of the financial sector where it is now a requirement for publicly traded companies in the U.S. to implement an internal control report on the adequacy of their control over financial reporting, this includes data that might affect financial statements.
Other regulations include the Sarbanes-Oxley Act, the Federal Information Security Management Act, and the EU Data Protection Directive. The latter is a harmonization of national laws designed to protect Personal Data and is of great concern to multinational companies due to its extraterritorial effect. Failure to comply with these laws can result in a wide range of penalties from fines to imprisonment and in turn there is a resultant increase in the demand for specialty skills and qualifications in cyber law and IT compliance. This increase in legislation has led to a greater awareness in cybersecurity issues at Board and executive level and a demand for qualified professionals in the cybersecurity industry.

7 . Collaboration and Information Sharing

Hopefully the coming years will see ever more effective collaboration in the cyber security domain, where collaboration combines the power of unity with the flexibility to innovate, and information sharing is not constrained by perceived barriers between intelligence and operations.

An excellent recent example of collaboration has been in the banking industry, where various banks have worked together and with the global law enforcement community to take down the computer systems used by the gangs behind the ZeuS and SpyEye banking Trojans. This took place in the UK, USA and other countries, and involved intelligence sharing and best practice advice and support to those affected by the malware.

Another context for collaboration is within industry sectors, where competitors can share information on the specific threats they face, but at the same time have confidentiality on their commercial intellectual property, or data on the specifics of incidents which affect them. This can help bolster security in an industry sector as a whole, and has given rise to various industry collaboration initiatives.

Tied to this, academia can be involved, with UK Research Councils having made investments of Â£10m in cyber security research, and a Â£3.8m Global Uncertainties programme on digital dangerous digital devices.

Public-private partnerships can vary widely in their specific approaches, but generally involve some combination of sharing information, joint exercising, joint initiatives, and joint projects; where a project may be seen as an activity which is time-delimited and has a specific goal. An example was the UK Cyber Security Strategy, where Government funding worth Â£650m was announced, and partnership activity from the strategy continues through initiatives such as the Cyber Growth Partnership and the UK's Joint Task Force on Cyber Security.

In the face of rapidly evolving cyber threats, public and private organizations must bolster cyber security through cooperation and the exchange of data on best practices, threat intelligence, and indicators of compromise. The most popular context for collaborative information sharing is public-private partnerships. These partnerships can occur at the national, regional, or local level, and can greatly enhance the effectiveness of both public and private cyber security efforts.

7.1. Public-Private Partnerships

Between governmental and private entities to work together in the research, creation and implementation of security legislation and policies as well as the development of best practice guidelines. These partnerships aim to seek out and combine expertise from the public sector industries with those in the private sector to develop initiatives that will benefit the security of critical infrastructures and key resources, as well as the security and privacy of business entities and the general public. In the United States, the National Infrastructure Protection Plan (NIPP) and Homeland Security Presidential Directive 7 (HSPD-7) are two examples of how government and specific industry sectors have formed public-private partnerships to protect critical infrastructures. However, despite the NIPP and HSPD-7 being aimed at specific industry sectors, relevant learnings from these initiatives can be applied to other areas of cybersecurity to improve overall protective measures. Public-private partnerships are essential in identifying and mitigating vulnerabilities that could have potential adverse effects on public safety and national security.

7.2 Sharing Threat Intelligence

Primary research found that loss of valuable proprietary information was the biggest concern with sharing threat intelligence. This was confirmed in an interview with the head of Europol's Cybercrime Centre, who revealed that businesses are often unwilling to share information due to fears of reputation damage. As discussed in sections 5 and 6, this proprietary information is generally related to indicators of compromise that organizations are often unaware of, which is causing internal and external threat actors to easily exploit systemic vulnerabilities. Indicators of compromise are pieces of forensic data that are left on a hard drive, memory, or network that can identify an intrusion attempt. Organizations are still hesitant to share this information as they believe it will damage their reputation and is often seen as giving an advantage to their competitors. This is reinforced with findings that organizations see brand protection as the main driver for security spending. If information sharing on cyber threats is to be improved, it will be essential to ensure that shared data is not leaked and that it does not have a negative impact on the affected organization. It must show immediate and long-term value for an affected organization. Considering the legislation issue in the US, it is apparent that some companies still see getting to know their breaches as a legal liability, which results in failure to report breaches and share data. This issue may be difficult to overcome unless there is a change in public policy and opinion. A new survey of government officials of G20 countries revealed that they felt international cooperation on cybersecurity was poor and that they were not convinced of its long-term benefits. This again relates to section 5 findings that show there is a lack of incentive to address a problem that is not seen as an immediate threat. A significant international shift in opinion will only occur if the long-term benefits of cybersecurity are known and this will likely require a demonstration of its effectiveness through improved information sharing.

7.2 Industry Collaboration Initiatives

Today's cyber security threats are becoming ever more complex with technological advancement, leading to

a greater need for collaborative industry initiatives so that the private sector can keep up with the advancements and increasing capabilities of adversaries. The cyber security industry initiative is one such initiative, where members agree to specific activities that advance cyber security. These initiatives may take many forms, including research and development, the promulgation of best practices, or other activities that serve the ultimate goal of enhancing cyber security. The cyber security industry initiative has many important dimensions and this risk paper touches on a few, with the hopes of delving deeper in future works. One of the most promising is the increased focus on cyber security in the context of public policy advocacy. This involves industry/government collaboration to shape public policy in ways that improve security. In the US, this is likely to involve legislation encouraging greater cyber security in critical infrastructure sectors. An example of industry initiative in this area is the cyber security steering committee, an internal task force at the IT sector of the European commission, TECIP. A more ambitious and strategic initiative is an attempt to drive and coordinate a major paradigm shift in cyber security research and development. This is an area where the IT sector could learn from the US defense sector's successful in the past 3rd offset initiative. In the context of EU cyber security policy, it might be possible to achieve coordination between public and private investment to reach the critical mass required to make Europe a leader in cyber security. Finally, industry initiative includes the mobilization of specific sectors for collective action, often seeking to address equally specific issues. An example might be the finance sector seeking to coordinate information to better defend against financially motivated cyber-attacks. This is an area where there are many possibilities and also much diversity in the ways that cyber security industry initiative might help improve cyber security.

8. Emerging Technologies and Trust

One way to address the credibility issue is to employ emerging technologies to provide credible evidence of past actions. Traditional security data is fine for checking if something is bad (e.g. has this application been seen doing something malicious?). It is less useful for checking if something is good, and of no use when trying to convince a skeptical party. Imagine a situation where an employee is attempting to circumvent organizational policy because they feel the policy is too strict. Their manager has a SIEM solution that shows an alert for policy violation. However, the employee can simply claim that this was a false positive and there is no way for the manager to objectively prove the employee wrong. On another front, consider incident response. When an analyst is trying to work out how an attacker got into a system, what they did and what systems were affected, it is all too common to have to give up and tell the boss and affected system owner that "we may never know exactly what happened". In both cases what is lacking is credible evidence. In the first example, what would convince the employee his action was caught and was really a violation was if the SIEM could show a playback of exactly what policy was in effect when the SIEM rule was created, perhaps supplemented by a keystroke video with all sensitive data obscured. This would not only convince the employee, but also provide the analyst with a concrete roadmap of what to look for. In the incident his team would have a far easier time restoring the systems to their original state so they can isolate compromised data and perform forensic analysis. What would make this possible is the use of data from the Machine's learning (ML) algorithms present in many AI tools, to automate tasks that would previously require human initiative and to solve those problems in a manner similar to how a human would do it. This automation frees the human operators to play a higher level supervisory role where they can focus on the questions that the ML automation is unable to answer. An example at the higher end of the security food chain is an organization defending against a skilled and persistent attacker. The defenders would like to know how their best defensive posture stacks up against the attacker across the kill chain, whether the attacker is being deterred and if so how they can force them to disengage. The ideal scenario is to play out a game of wits, with the humans supervising the AI agents as the action unfolds and debriefing afterwards. It is great for security, but whether it will ever be acceptable from an ethics and accountability standpoint is uncertain. High level human supervision is also desired for the recent crop of chat bots and other AI agents that attackers are beginning to target for social engineering and secondary malware infection.

8.1 Artificial Intelligence in Cyber Security

Various flavours of artificial intelligence (AI) are being used for automating cyber security processes. AI technologies have been applied to all kinds of cyber security problems. For example, fuzzy logic has been applied in anti-virus software; genetic algorithms and neural networks have been applied in the development of new intrusion detection systems; and data mining techniques have been used for identifying patterns in network traffic, a common technique of worms and other self-propagating malware. AI has been used in these ways to automate traditionally manual or semi-automated cyber security tasks. If successful, this

should lead to freeing human workers from mundane work and providing them with the ability to deal with complex security problems. The main limitation to date has been that AI technologies often require large amounts of training data (for supervised learning), or high-quality data for the automatic generation of models. It is only a well-resourced organization that can currently afford to do this, and data quality is often lacking. AI has seen more controversial uses in cyber security. In particular, the development and sale of so-called 'cyber weapons' a hot topic in world security today. This can be attributed to the widely publicized successes of the US and Israeli Stuxnet worm. It is known that various organizations, including both defense departments and private companies, have used AI to develop malware that is specifically designed to be autonomous and adapt to its environment. This malware is akin to a 'Swiss army knife', being able to perform a wide variety of tasks in an automatic fashion. The US Department of Defense has been using AI in a more passive manner for identifying and prioritizing vulnerabilities that have been uncovered during network penetration tests. All this activity is a cause for concern, as it greatly escalates the cyber arms race, and this kind of malware easily has the potential to cause collateral damage to uninvolved parties.
Nevertheless, we are confident that the development of AI for defensive cyber security outweighs the offensive uses. This AI arms race is a natural progression of the automation of security systems, and malware is best fought with self-defending auto-immune systems.

8.2 Blockchain Technology for Trust Assurance

Cryptocurrencies and blockchain emerged as the outcome of the global financial crisis in 2008 to produce an option to the traditional banking system. Blockchain technology can provide a new tool to help in securing the IoT. In a paper by Xu et al., the authors acknowledge that current technologies cannot satisfy the requirements of decentralized security, managing the access and availability of data, ensuring the integrity of data and systems, and attaining true accountability in data operations. The essence of blockchain is to provide a decentralized environment for the storage of data which can be securely accessed and managed by its stakeholders. Nodes in the blockchain must reach a consensus before updating the database in the distributed manner constituting the blockchain. The aim is to create a trustworthy ecosystem where the data in storage and in transit can be vetted and its integrity can be assured. A suitable structure for implementing blockchain has been shown in research by Dorri et al. for the IoT. This strategy integrates the use of smart contract at the edge of the blockchain to have a lightweight consensus for the devices. The architecture involves the use of a semi-permissioned network by the devices to efficiently assimilate their data into the blockchain so that it may be processed by a central party. This system is ideal for the query and processing of consumer IoT data to understand the behavior of the devices and the needs of the to improve their user satisfaction as it ensures the integrity of the analytics data.

8.3 Internet of Things (IoT) Security

Although IoT devices can potentially increase the quality of our lives by a significant degree, an alarming problem is that they often handle large amounts of personal data. According to an HP study, 70% of the most commonly used IoT devices in the home contain vulnerabilities to cyber attacks (Internet of things: A survey, 2016). This is an issue that affects consumers. It's bad enough when one PC is breached, but when there are potentially dozens of smart devices in a household all collecting different types of data, if one of those was to become compromised the implications it has on the rest of the network and data associated with it could be substantial. This could be anything from the loss of personal identity data or in a more extreme case, if an IoT medical device was to become compromised it could put someone's life at risk. The same issues apply to Industrial and organisational systems. With an increasing drive to automate industrial

Systems using IoT, the consequences of a security breach can be much more severe than the attacks on data from current PC systems.

The Internet of Things (IoT) is becoming an increasing topic of interest in security, with rapid expansion in the number and type of "things" being connected. The need to address the security of IoT has never

been more relevant. A recent study suggested that over a quarter of identified data breaches will involve IoT, although the amount of IoT investment is ever increasing (Gartner News Press, 2018). Fujitsu has also recently stated that IoT security has significant implications for trust, a drive to test and develop a data tracking standard using Blockchain in Data services (Fujitsu, 2017). The idea of IoT is to have devices that are ultimately smarter and making our lives easier, however the issue that arises is the inclusion of these devices in critical systems (e.g. healthcare, transport) when they are not built with security in mind.

9. Future Trends and Challenges

Schema for the guideline 2, 3, 4, 5 is: There is no one-size-fits-all solution to cybercrimes and risks. Like technology, the cyber threat environment is always evolving. With the growth of the Internet of Things (IoT) and interconnected devices, conventional hacker strategies are going to be more powerful. This will raise the likelihood of successful cyber attacks due to the wider attack surface given the increasing amount of devices that hold private data and are connected to the internet. The rapid development of technology in areas such as machine learning, AI, and augmented reality will also produce new security gaps that will need to be addressed by cybersecurity professionals. In order to remain ahead of cybercriminals, it's crucial that cybersecurity aids are also positioned ahead of the technology trend curves. An increase in data and consumer digital footprints will see a rise in the amount of private info that can potentially be stolen. The introduction of systems such as the European Union's General Data Protection Regulation (GDPR) is designed to shield personal data and impose stringent guidelines on data protection for companies both inside and outside the EU who offer goods or services to the EU. Measures and implementations such as GDPR are good for consumer data protection; however, they will essentially create a bigger incentive for hackers to steal and exploit personal data. This will add pressure on companies to protect consumer data and may potentially lead to more properties of cyber attacks being aimed at companies who hold large databases of private data.

9.1. Evolving Cyber Threat Landscape

There has been a significant shift in recent cyber-attacks. In the past, cyber-attacks were more commonly associated with disgruntled employees and people seeking revenge, however this has changed. Cyber-attacks have become a method of choice for various individuals and organizations seeking to gain financially or further their own causes. There has been a vast increase in financially motivated cyber-attacks aimed at stealing personal information. Certain types of information are of high value to attackers, for example personal financial information, as it can be directly translated to potential monetary gain. Attackers can use various methods to steal this information, from deploying malware such as keyloggers or Trojans, to using more complex methods such as phishing or social engineering. Global events such as the COVID-19 pandemic have also been largely exploited by cyber criminals due to the increase in the amount of people working from home. This has created more opportunities for attackers as they take advantage of the rapid transition to new technologies and the vulnerabilities that come along with them. Attacks have become more sophisticated as well as more frequent and it is expected that this trend will continue into the future. As consumers and their data become more heavily targeted, it is crucial for businesses to adapt in order to protect their customers.

9.2. Balancing Convenience and Security

This will manifest itself with consumers questioning the security policies of service providers and an increased demand for security-incorporated features. Thus, forcing a change in the way IT services are marketed to the public.

As a result, consumers have become more wary when utilizing online services, fearing compromised security. This change in consumer mentality has led to consumers in the future seeking reassurance that their data is stored securely and with peace of mind that they are not putting themselves at risk by using certain services.

Cyber attacks on consumers are becoming more targeted and more effective, with identity theft and account

takeover incidents on the rise. Attackers are consistently attempting to monetize their activities with minimal effort. This has led to a rise in account hacking and fraudulent activity that has a direct impact on consumer finances.

The evolution of the cyber threat landscape has, in turn, influenced the digital age. The emphasis on digital services is leaving consumers open to attack. The convenience offered by modern technology allows consumers to access online services anywhere, at any time, using a multitude of devices. However, it has also increased the attack surface for cybercriminals, with a variety of new tactics that can exploit vulnerabilities to compromise personal data.

9.3. Maintaining Consumer Trust in the Digital Age

To address these strains to data security, the computing industry must place a significant emphasis on maintaining the trust of the consumers. Security breaches can have a profound impact on the trust of a company in the eyes of consumers. A recent survey conducted by the Business Software Alliance revealed that 79 percent of computer users in the United States are concerned that their personal information might be stolen online. A study by Gartner Group addressing the financial impact of publicized security breaches on enterprise IT organizations revealed that 80 percent of respondents believed that publicized security breaches had affected their company's bottom line. 60 percent of those reported that the effect was negative. These trends have an overall negative effect on e-commerce as a greater portion of the population comes to view online purchasing as untrustworthy and revert back to traditional methods. Data privacy and security are considered the most important issue to online consumers. 70 percent of the same BSA survey respondents said they would use the internet more if they were more assured that their personal information would be protected. These findings imply that companies must implement better security measures to sustain and attract new customers. Providing consumers with a greater sense of security in their products is an opportunity for differentiation between competitors. This can result in greater customer loyalty, particularly when a company's security reputation is good. For instance, in the credit card industry, many consumers have come to learn which banks have lesser incidents of stolen card numbers and identity theft. This knowledge could potentially affect choice in credit card and also, which online payment services to use.

Conclusion

In conclusion, linking back to the two implications of consumer trust in e-commerce and e-government, it is evident that the level of online consumer trust remains largely low. The findings narrowly supported the first hypothesis, that "Consumers who are more security-conscious are less likely to conduct online transactions than regular consumers." This indicates that consumers who are aware of potential security threats are less likely to trust in the safety of e-commerce and are less likely to engage in it. Although security-conscious consumers consider the SSL indicators and website reputation ratings of a company, the common transaction medium of credit card payment still remains a large area of risk and diversity in trust. With the wide acceptance of SSL security measures among companies, consumers have a consistent means of evaluating the trustworthiness of different companies' practices. This is not the case for payment by credit card, where different companies and banks have varying security measures and policies. Government websites and information handling are usually held in high trust regard by the public. It was thought that higher consumer confidence in the security of transaction and information handling with government institutions would lead to a higher likelihood for citizens to engage in e-government between secure trusted government sites and the secure reporting of personal information. This was not supported as there was no significant difference in consumer trust in government site transactions and citizen ID input, and the overall consumer trust in e-government.

Findings

The findings are extremely interesting and insightful, providing clear evidence that cyber security does strongly influence digital consumer trust when visiting and using a website. When comparing the experience of the two groups, those who had been victims of hacking before and those who had not, there is a clear difference in trust and perceptions of the various elements of security present on a website. Primarily, victims of hacking claimed to trust websites less, and this was particularly the case in more inexperienced surfers. This is reflected in the fact that relatively low-experienced surfers who have been the victims of hacking have significantly lower perceptions of security while visiting a site. This insight provides a clear link between cyber security and digital consumer trust, which is further evidenced by experience differences on the perceptions of various security elements on a website. Victims of hacking with less experience were found to be more conscious of the security at the point of entry on a website, as well as being more risk-averse and spending more time to find trust indicators such as a trustmark/logo and guarantee or security policy page. This would lead to the conclusion that cyber security plays a significant role in determining digital consumer trust regarding site security, as consumers, particularly those with experience, felt the effects of poor cyber security and have since become more aware and cautious of online security measures.
This study has resulted in a number of interesting findings, which are spread throughout each stage and sub-stage of the model. These findings allow the model to be completed, providing insight and evidence into the determinants perceived of digital consumer trust when using e-commerce and the specific role cyber security has in influencing this. Each sub-stage finding will be discussed, explaining the results and analysis of the study in terms of cyber security and digital consumer trust.

References

With the increasing use of the internet and the move from physical to virtual customer relationships, trust has become a key concern for businesses and consumers alike. While businesses are focusing on building consumer trust to gain a competitive edge and greater revenue through stronger relationships and repurchase intentions, relatively little research has examined the implications of trust for consumers in the online shopping environment (Gefen, 2000). This oversight is particularly notable in the area of trust and the customer in a B2C context, where the general consensus is that trust (in a vendor) has a significant effect on purchase intentions and actual purchasing behavior often mediating relationships between marketing, price and advertising (Ganesan, 1994). A variety of studies have shown the importance of trust in a vendor for consumer purchasing behavior online (Lee, Kim and Kim, 2009; Kim, Ferrin and Rao, 2008; Jarvenpaa, Tractinsky and Vitale, 2000) however no study has yet looked at how trust in a vendor translates to trust in the vendor's website or how cyber security's influence on this trust. This essay will address this research gap looking at cyber security's influence on consumer trust in a B2C context and the implications this holds for businesses who are seeking to gain a competitive advantage over rival firms with the aim of improving consumer purchasing behavior.
href="https://en.wikipedia.org/wiki/Consumer_confidence">Consumer confidence.
href="https://en.wikipedia.org/wiki/SQL_injection">SQL and file upload.