國立交通大學

企業管理碩士學位學程

碩士論文

# 個案研究：在駭客事件下，IP攝影機產業中的應對組織策略選擇準備

# Organizing Strategic Choices in Preparation of a Hacking Incident in the IP Camera Industry: A Case Study

研究生: Justin James Allan Pryor 班恩傑

指導教授: 黃仕斌

中華民國 103 年 6 月

# 個案研究:在駭客事件下，IP 攝影機產業中的應對組織策略選擇準備

# Organizing Strategic Choices in Preparation of a Hacking Incident in the IP Camera Industry: A Case Study

研究生: 班恩傑 Student: Justin Pryor

指導教授: 黃仕斌 Advisor: Dr. Kevin Huang

國立交通大學

管理學院

企業管理碩士學位學程

碩士論文

A Thesis Submitted to Master Degree Program of Global Business Administration

College of Management

National Chiao Tung University

In Partial Fulfillment of the Requirements For the Degree of Master in Business Administration

June 2014

Hsinchu, Taiwan, Republic of China

中華民國 103 年 6 月

## Abstract

The purpose of the paper is to present a list of possible actions to take in the preparing and reacting to a hacking scandal event taking place in the Internet protocol camera industry. This paper begins by exploring the background of the public relations field of research. This is important to show the basis for the study that this research envelops. It then goes on to explore the background of hacking in the world and what this entails. Hacking takes on many different forms and is undertaken due to many different kinds of motivation.

The paper discusses Grunig's four models of public relations and how they are applicable to the modern world. It goes further into looking at the four-stage action plan set out by Alfonso Gonzalez-Herrero and Suzanne Smith for dealing with crisis management in the age of social media.

A case study of hacking incidents relating to the Foscam and TRENDnet companies in the past few years was conducted in order to explain the cause and justification for this paper's topic of research. The reader can see the results of what happens when IP camera companies do not have a proper public relations crisis management action plan in place to deal with a hacking scandal.

The case study's findings lead to the development of a plan of action for potential industry insiders to use in the future to assist them in preparing for and reacting to a hacking event. This research works on the basis of Gonzalez-Herrero and Smith's generalized action plan that is in place for crisis management. The researcher set out to make an industry specific version of this work while also adding in other elements of Grunig's research and the researcher's own contributions. The conclusion finalizes the need for such an action plan and states that it is unproven, so caution is necessary when constructing a real-life plan of action. The conclusion suggests that there are many benefits to employing the results of this research paper in the IP camera industry.

## Acknowledgements

- I would like to express my sincere gratitude to Kevin Huang for providing a very supportive environment in both his classes and throughout the thesis writing process. Having a teacher like him is truly an inspiration for any student.

- I would also like to thank CT Yang for providing me work experience in the IP camera industry and giving me a first-hand education about how the industry works. His help has truly been an education all on its own.

- A final note of thanks to Professor Jinsu Kang and Vanessa Chung for all of their help and assistance throughout the course of this degree. They often went above and beyond what was required of them when lending help to students.

## Table of Contents

Abstract……i

Acknowledgments…….....ii

Table of Contents……iii

I. Background and Problem Statement……1

II. Public Relations and the Four Models of Public Relations Theory ……...4

III. Research Methodology……15

IV. The Case Study: IP Cameras and The Invisible Intruders……...17

V. Action-Plan for Hacking Event of IP Camera Company……..34

VI. Conclusion……...39

VII. References……..40

VIII. Appendixes……...47

# I. Background and Problem Statement

## 1.1 Background

The field of public relations study goes back to around 1900 with the establishment of the Publicity Bureau. Many academics consider this to be the first big step towards actually documenting the process of how to perform effective relations between organizations and stakeholders. Although earlier efforts at various forms of public relations existed, this was the first step to officially establish it as an academic field.

World War II led to the mass development of propaganda between belligerent countries. Once the war finished, these new experts moved into the private sector. This ushered in the beginning of corporate public relations as a profession in itself. With this movement came the beginning of trade associations, public relations agencies, public relations magazines, and official academic study of the subject.

Following this, Rick Levine, Christopher Locke, Doc Searls, and David Weinberger released another piece of literature, called'The Cluetrain Manifesto.' At the time, it seemed controversial for its views predicting the future of public relations linking to social media. However, it was proven valid just seven years later in 2006, as the full might of the internet age came to bear its power. This manifesto was a collection of 95 theses put together into one document describing how businesses must adapt and change their public relations style to the new Internet age. (Levine, 2009)

Although there have been many papers on public relations since these pieces of literature, there is still room for improvement. Public relations itself is a very wide-open field and until 1984 had no clear direction. With the coming of the Internet heralding many new methods of communicating with stakeholders, there will surely be more significant papers to come. Grunig himself has made a few attempts to update his work in

order to accommodate the social media boom. A major work that he created is an article called “Paradigms of Global Public Relations in an Age of Digitalization.”This paper delves further into techniques to improve communications and strategies for public relations using computer sources of technology.(Grunig, 2009)

Although these papers tend to cover very broad ranged strategies and subjects, they still give a general guideline towards how to properly handle a company’s public image. There is a new facet of public relations that has yet to be significantly covered, yet is very relevant to the business world:how to respond to hacking scandals. There have been countless examples in the past decade of companies losing important vital information due to advanced hackers (or even sometimes simple mistakes or lack of foresight in IT structural defenses). Certainly, the best way to avoid the question of how to deal with stakeholders in the case of a hacking scandal is to increase defenses to the point that they do not occur. However, this is not always possible and if it is, is prohibitively expensive. The pace of technology is also occurring at a breakneck pace. With some hackers being at the forefront of this technology, preventing them from accessing some systems is nearly impossible. This begs the question of how to respond to hacking incidents from a public relations perspective. It would behoove all major companies to have backup plans for if and when these events take place.

Another form of hacking, although having occurred for several decades, is much less popular. Some hackers break into systems just for the sake of being able to do so. Their motivations are multiple but this style of hacking does not end up in monetary gains. This is a whole other challenge to deal with. Oftentimes these hackers are motivated simply by hacking the ‘unhackable.’ When a company states their software or servers are untouchable, this has frequently led to an *increase* in hacking attempts, simply because of bragging rights for the hacker that successfully completes their mission. It seems that building up defenses against Internet hackers is a double-edged sword. By publicly stating that a company has an extra-ordinary level of security invites the most advanced hackers to break into their systems.

One such example of these styles of attacks is in the Internet protocol (IP) camera industry. This is a relatively new type of product that only in recent years has become popular. The industry is too infantile for many studies to have been performed on it, especially relating to hacking events.Furthermore, if hacking incidents from the last two years are an indication of the future of this industry, all IP camera companies will need to brace for not only hacking attempts, but also with how to deal with the blowback from the worst case scenario of actually being breached. *The previous frameworks for public relations when discussing IP cameras specifically needs to be approached and modified to effectively minimize problems after hacking events occur.*

## 1.2 Goals and Objectives of the Research

The goal of this research is to present an alternative framework specifically for dealing with choices in public relations pertaining to IP camera hacking incidents. Public relations is a vast field with many different aspects to it. Most major research has presented somewhat generic theories and frameworks for how to deal with the many aspects of the area. Being able to have more information and knowledge on how to react when specific events occur is thus a valuable addition to the field of public relations research. This paper hopes to be able to present a viable framework for IP camera companies to utilize in case their products and infrastructure is hacked or exposed.

The research makes use of the '4 models of public relations' by Grunig. The updated research of Grunig, "Paradigms of Global Public Relations in an Age of Digitalization." as well as the 'The Cluetrain Manifesto' are both examined and analyzed to extract the more valuable aspects that pertain to this thesis' topic.

The research asks:

- *What strategies should a company employ in the case of an IP camera product being hacked in order to attain the lowest possible damage from the negative public response of the incident?*

# II. Public Relations and the Four Models of Public Relations Theory

## 2.1 Historical Background of Public Relations as a Science

In 1984, a significant work of literature came out from the author James E. Grunig titled 'Managing Public Relations.' Before this piece of writing, there were no major public relations papers being followed and quoted by people actually involved in the industry. It is now one of the most commonly referenced pieces in the public relations field due to its new theories and applications. In fact, Bill Sledzik, a public relations academic with over 15 years of experience stated that "Runig& Hunt's '4 Models' of public relations practice went on to become the most talked-about theory in the discipline." (Sledzik, 2008) Before this, there was a significant lack of theories related to actual practice of public relations. As such, in many instances significant errors in judgment were made as the people performing press releases and communications with the public were undisciplined in their actions. Many instances can be found in the last 30 years where companies made significant errors in judgement related to their public relations efforts. The main contribution from Grunig's work has been the '4 Models' of public relations. The four facets of his work included press agentry, public information, two-way asymmetrical, and two-way symmetrical categories of models

## 2.2 Grunig's Four Models of Public Relations

### 2.2.1 Press Agentry/Publicity Model

This model is described as being a one-way communication between companies and the public. It "describes propagandistic public relations that seeks media attention in almost any way possible." (Grunig and Hunt, 1984)This model attempts to persuade the public into believing what the company wants them to think.

This is also classified as being under the 'one-way communication' category. Press releases and other information being sent out from the company only goes one way. The response from the public is of no concern and is only adjusted in the future with

more positive information. One-way models of communication under Grunig consist of a lack of effort on the company's part to research or discover any opinion of the public. The emphasis on this type of model is the search for media attention and often involves are different or highly memorable to the public.

A modern example of this is PETA's (People for the Ethical Treatment of Animals) campaign to discourage the purchase of fur in the general public. A particularly famous campaign they employed was entitled 'I'd Rather Go Naked Than Wear Fur.' This controversial campaign was high-impact as it involved pictures and videos of naked celebrities using catch phrases such as 'Ink not mink' and similar rhymes. It was successful in that people easily remembered the images and the messages that they bore. This is an example of press agentry because the image aims to create a viral result, while only projecting one aspect of a very complicated issue. (Wang, 2009)

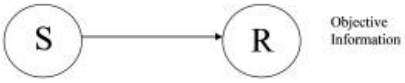

- Source: Stevenson (2009)

**2.2.2 Public Information Model**

This model also functions as a 'one-way communication' model in that messages are only sent one way and responses are disregarded.Usually to perform this function, in-house staff is employed to constantly create company-positive information and articles for use to disseminate to the public at large. Note that this image almost always only contains positive news, with a severe lack of negative news being communicated.

A modern example of this isthe Infect TRUTH campaign that was aimed at informing public about the contents of cigarettes. Tobacco companies had been using the chemical urea in their products and this campaign wanted to highlight that in an informative, yet memorable way. They recorded a phone call between a paid actor and a

tobacco company executive offering to sell them dog urine, as it contains the same chemical. The campaign aired on many radio stations in its unedited form. This is an example of public information as it attempted to educate the public about the truth of what is contained in cigarettes, in a very informational fashion. (PR Group 13, 2009)

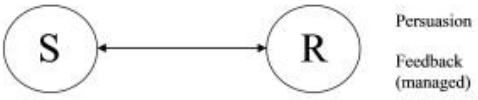



- Source: Stevenson (2009)

### 2.2.3 Two-way Asymmetric

The two-way asymmetrical model revolves around casting a view of a company's image/information on the public. Although it does employ research and other methods to attain public reactions, this is not the focus. The focus is to impart the desired image on the public through the use of manipulation and accurate targeting in both the audience and their beliefs. Gauging the reaction of the stakeholders is not of utmost importance in this model, but is a part of it nonetheless.

Most modern advertising takes the form of this model. Marketing campaigns are now almost always highly targeted at specific audiences and aim to display a very precise message to that audience. The two-way communication comes through research into the target market. The company and its marketers actively seek their opinions to discover what needs and likes that they have. They then work to provide that image of the company. It is asymmetric since the company only uses the feedback of the consumer as a guideline to present its public image, not to actually change the actions of the company.




- Source: Stevenson (2009)

### 2.2.4 Two-way Symmetrical

Being the only one of the four models that uses two-way communication as its basis, the two-way symmetrical model is touted as the optimal method for a company to employ by Grunig. Companies that operate their public relations using this method use scientific research to identify the messages "most likely to produce the support of publics without having to change the behavior of the organization."(Grunig, 1992)

It involves a lot of active communication with stakeholders in every area, including employees, investors, customers, etc. Misunderstandings are sought out and resolved by communicating with all stakeholders to develop the best-case solution.


- Source: Stevenson (2009)

With the advent of the Internet age, this form of public relations is getting easier to perform. Great examples are through the use of social media and blogs. Many large companies employ social media managers whose sole purpose is to respond to queries and comments made on a company's social media websites. Some more humorous versions of this are large restaurant chains such as Burger King and Taco Bell who often respond in limericks and jokes as a way to differentiate themselves and their public image.

### 2.3 Summary of the Four Models

In common practice, the frequency with which each model is used is based on a variety of factors. Press agentry used to be a very common form of public relations as many companies and organizations tried to impose their brands and images upon the public without caring about the reactions.

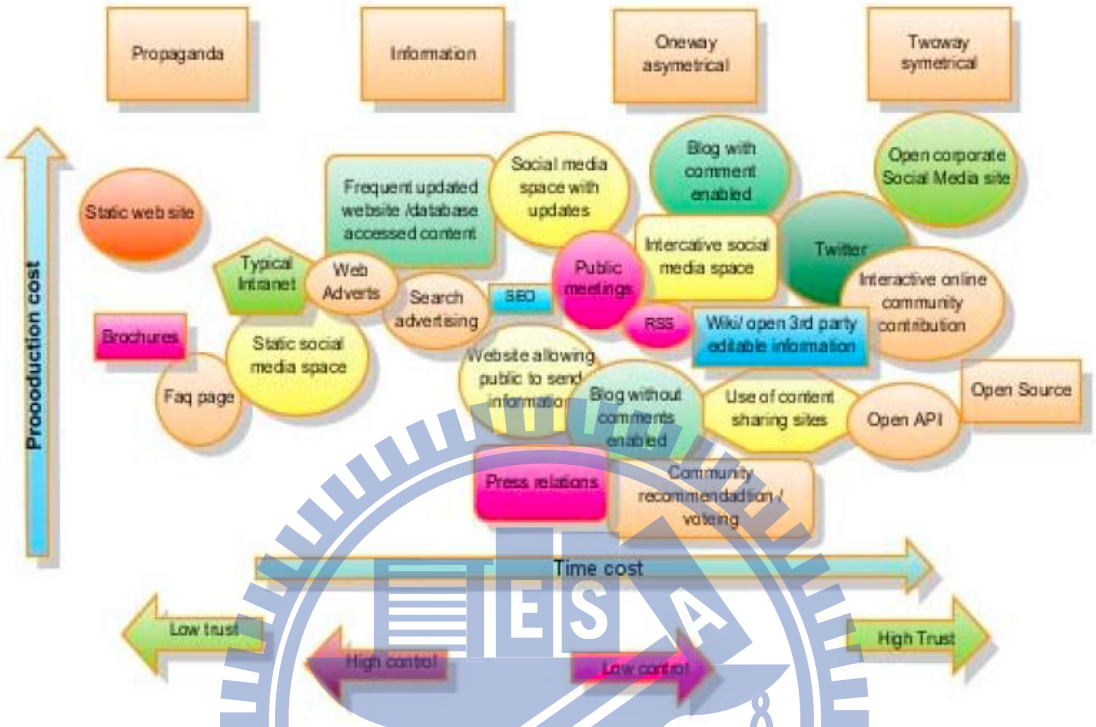
Public information has tended to be utilized by non-profit and governmental organizations more and more as history has progressed. These organizations often have a large amount of bureaucracy; yet have a moral and sometimes legal requirement to present the truth when dealing with the public.

One-way asymmetrical communications is commonly practiced nowadays and since the age of the marketing and public relations firms being developed. They currently have access to huge amounts of data and can use this information to present a more focused and efficient image.

Grunig touts the two-way symmetrical model as being the best model for a variety of reasons. He believes that it represents the best way to come to a positive outcome by collaborating with stakeholders on all facets of an organization's activities. This is a particularly time consuming and often difficult public relations model to follow. However, with the advent of social media it is certainly becoming easier to implement.

The following chart shows a compilation of methods of communicating with the public in the current age. It ranks each method based on its respective money cost and time cost as well as categorizing them based on the four models.D. Phillips developed this chart based on the work of Grunig and his own views. It is a good tool for use by organizations in deciding what kind of model they want to use and what the particular costs will be in relation to that activity.

***Pictured: Types of Social Media in Public Relations***




- Source: Phillips, D. (2009)

## 2.4 Crisis Management and Using the Internet in Public Relations

In order to delve further into how to properly respond in the case of a hacking incident, it is important to examine recent research around the topics of crisis management in the use of public relations.

*"In only a few years the Internet has evolved to become the most popular way to communicate with customers, investors, analysts, employees, the media, and the many other stakeholders any company has, transforming the practice of corporate communicators and public relations professionals."*

- Alfonso Gonzalez-Herrero and Suzanne Smith (2008)

Gonzalez-Herrero and Suzanne Smith have examined this specific subject in their paper entitled 'Crisis Communications Management on the Web: How Internet-Based Technologies are Changing the Way Public Relations Professionals Handle Business Crises.'They have put forward a strategic general framework to deal with the public in case of crises.

Their work stemmed from the lacking of a specific framework that collected all of the available information and gave practitioners a specific plan to use. The need for this had become apparent as the world moved into the Internet age as many companies were making simple mistakes when it came to communicating with their customers through social media. Traditionally, this was not as much of a problem since "up until very recently, companies used PR to address their audiences through mass media such as TV, radio, newspapers and magazines." These forms of media allowed companies to project what they wanted to project and involved little to no feedback from the stakeholders. Most companies preferred this as it let them control their image more easily and also cost less at the same time. However, this led into bad situations when crises occurred as these companies did not know how to properly respond with no available feedback.

Companies now need to present a transparent and open flow of information between their customers. People respect and require this from businesses that they want to work with. This is especially true when bad situations happen, particularly if it is the company's fault. Having a framework on how to react is vital.

Gonzalez-Herrero (1994) and Gonzalez-Herrero and Pratt (1995, 1996) created a four-stage model to deal with crisis management. It was based off a life cycle of a natural organism in that it is born, grows up, matures, and then dies. They applied the same theory to the birth of a crisis in the real world. Their four stages were titled issues management, planning-prevention, the crisis, and the post-crisis. In the 2008 paper mentioned previously by Gonzalez-Herrero and Smith, they have analyzed and updated the four-stage model to include the new media tools that are available.

The issues management stage consists of the following action plan:

> *1. Assign resources – human and economic – to issues management tasks. Consider whether an external agency or service can be of help.*
> *2. Establish an efficient online monitoring alert system that includes monitoring of websites, blogs, newsgroups, etc.*
> *3. Train the team. Become familiar with how things develop in the virtual world.*
> *4. Draw a full map of online influencers showing issues of interest or concern.*
> *5. Prioritize your actions on issues based on their probability of occurrence and its possible impact on the organization.*
> *6. Consider starting a corporate blog to engage with the online community well before a crisis situation arises.*
> *7. Think globally. Any local issue in the Internet can today easily evolve into a regional or a global crisis.*
> *8. Draw up guidelines on the approach, tone, and language that is appropriate for dialogue in a dynamic, online environment. This will be quite different from the more formal and distant corporate tone and language used in traditional communications.*
>
> - (Gonzalez-Herrero and Smith, 2008)

Their suggestion for the planning-prevention phase is as follows:

> *1. Consider developing the crisis manual online: it is easier to update and maintain than hard-copy, and it offers the possibility to include links to multiple sources of information and databases. It also allows communications actions such as e-mail distributionand point-and-click distribution of press materials.*
> *2. Update e-mailing lists and contact databases.*
> *3. Check whether the regular media monitoring service is fast enough to follow the crisis, especially for online media outlets.*
> *4. Register all possible domain names, including those with negative connotations, to prevent registration and use by activists groups.*

*5. Draft guidelines to respond quickly to web-based rumours.*

*6. Consider the creation of an extranet or a webbasedwiki or team-room that could be used by crisis management team members to obtain internal information related to the crisis, guidelines, plans, news reports, statements, contact information,etc.*

*7. Provide guidelines to using the company's intranet to keep employees informed.*

*8. Create a hidden or a 'dark' web site that could be used externally in case of a crisis to update all constituencies about the issue.*

*9. Prepare links to be used on the company's web site, connecting visitors to other relevant sites, additional information, or useful resources.*

*10. Identify relevant third-party organizations and individuals (e.g., some bloggers) that could act as allies and can provide a balanced view in the case of a negative audience debate. Engage with them in advance.*

*11. Include a web expert and/or a blogger in the crisis team.*

*12. Evaluate your in-house capabilities to develop graphic, video, and audio files that could be quickly distributed online, whether they are simple digital pictures or more elaborate podcasts. Purchase the necessary equipment or think about outsourcingthese services.*

*13. Consider whether you need your traditional PR firm to do online PR or you need to hire a separate PR firm or partner that specializes in online PR.*

*14. Test the online crisis plan.*

- (Gonzalez-Herrero and Smith, 2008)

For the crisis portion of their research, they suggest the following list:

*1. Ensure your mainstream media and online monitoring services are aware of the crisis situation and that they report electronically all outcomes as they appear.*

*2. Use search engine optimization to make the company's web site appear at the top of a search.*

*3. Place an obvious link to crisis information (or your previously 'hidden' site) on your home page as soon as possible.*

*4. Use links to reputable third-party endorsements or to web sites that have favourably covered the issue.*

*5. Use the Net as a third-party information resource that reinforces your company's view. For example, you can take advantage of online tools like blogging.*

*6. Use the web for further information or instructions to consumers and the audience (e.g., In the case of a product recall, etc.). Make sure announcements are clearly seen from the home page.*

*7. Use interactive tools such as mini surveys to understand the audience's perception, including questions or comments such as 'what's your opinion?', 'we appreciate your view'. . . although take into account that such messages will need a response.*

*8. Consider whether chat tools should be used to foster dialogue – or suspended, due to the delicate nature of such situations and the anonymity that most of these tools allow.*

*9. Get CEOs to use the Internet to personally address stakeholders, something few of them do, according to Stock (2003).*

*10. Combine the use of online media with traditional media. Certain traditional media gatekeepers still confer a certain degree of credibility to a message that many online media do not yet have.*

- (Gonzalez-Herrero and Smith, 2008)

For the last portion of their recommended actions to take during the post-crisis phase, they wrote:

*1. Continue tracking the issue by monitoring blogs, online media, etc. during the*

*months – and even years – to come.*

*2. Thank those who helped the company during the crisis. From an online point of view, this could include 'thank you' e-mail messages or a 'thank you' message on the company's web site.*

*3. Update the company's online newsroom appropriately.*

*4. Define the strategies and tactics at play to rebuild the company's reputation: from in-depth analysis of Internet content and opinion leaders, to online chats with the most active bloggers.*

*5. Evaluate what happened and how the organization responded, so that the crisis plan and all the online related measures could be properly adapted.*

- (Gonzalez-Herrero and Smith, 2008)

## 2.5 Summary

The research performed by Grunig, Gonzalez-Herrero, and Smith have encompassed a very good basis for how to prepare for specific public relations crises in the modern age. This paper aims to further customize their work into the area of crisis management and response when hacking events occur in the IP industry. The author could find no work in the public relations field that dealt with this very specific topic and hopes that this paper can contribute to the field by presenting a specific list for companies in this industry to follow. It is based upon both the Four Models of Public Relations and the Four Stage Crisis Management Model and is aimed at a very specific target of the IP camera industry.

# III. Research Methodology

## 3.1 Research Approach

This paper takes the form of a case study. It was chosen because of the specific nature of the subject of this thesis. By examining the real-world situation on which this topic is related to, a reader can garner a better understanding of the value this researcher is attempting to provide. The aim of the research is to provide a specific action list to users that may deal with hacking incidents in the future of the IP camera industry. Being prepared in advance for this can save a company valuable time, money, and reputation.

The subject of the case is Foscam and TRENDnet, two IP camera companies that were hacked in recent years. They were also the only known ones to have made it to the news so far at the time of this writing. The author is of the belief that the nature of this industry will most-likely lead to future hacking events, and thus a need for this research exists.

This case study builds upon the research of Grunig, Gonzalez-Herrero, and Smith. They have all published numerous research papers in the field of public relations, with perhaps Grunig being the most often quoted author in the field. The foundation of this research is based upon both the Four Models of Public Relations and the Four Stage Crisis Management Model. The intention is to provide an IP camera industry specific action list for stakeholders to utilize if needed. The author is unaware of any similar research at the time of this writing.

## 3.2 Data Collection

Data collection consisted of analyzing news articles, blogs, financial sites, company websites, and industry presentations for data relating to the case study. The quotes in the case study relay accurate information of the actual people involved in the case. Attempts were made to contact the two corporations involved in the case, but

responses were unforthcoming. This may have been due to the negative nature of the subject of inquiry.

A large amount of public relation studies was read in preparation of providing the final action list for response to this case study. Grunig, Gonzalez-Herrero, and Smith's papers were of utmost relevance to this subject, and were vital in preparation of the author's work.

## 3.3 Research Limitations

The author attempted to remain neutral in all passages of this paper. It is a challenge to write a story while at the same time stating all the facts and figures in a fair and equitable fashion. The author ensured that his personal opinion was omitted from the bulk of the case study. This was necessary to produce an unaffected opinion in the potential reader of the case study.

As this is a case study piece of research, it should be said that direct theories, inferences, and discoveries of this research couldn't be expanded to the field of public relations as a whole. This research serves a specific and limited purpose as has been previously described. Further analysis and testing of the research would be required in order to prove this research correct and adequate for use in the real world.

## IP Cameras and the Invisible Intruders

*"Hackers are like kids putting a 10 pence piece on a railway line to see if the train can bend it, not realizing that they risk de-railing the whole train"*

- Mike Jones, security awareness division, Department of Trade and Industry, UK, interview) electronic vandalism (Warman, London Business School, interview)

In August of 2013, inside the quaint American city of Cincinatti, Ohio, the deep voice of a man was heard inside baby Emma Schrek's bedroom. Only this wasn't the voice of anyone familiar to the girl, it was a complete stranger from somewhere on the Internet.

The Schreks had invested in a relatively new technology called IP (Internet Protocol) cameras. When looking for a good baby monitor to use, they found that most in the industry were all limited to the home environment. They typically consisted of a video monitor attached to a speaker and microphone. They also usually came with some sort of remote device, normally a small video monitor that the parent could use to communicate with their baby. The transmission device is located inside the baby monitor, and the receiver can have either a small screen or just act as a radio.The main caveat with these devices is that they operate via radio broadcasting. As such, these devices are limited to the range of the radio, usually no larger than the span of the house.

***Pictured: Example of typical baby monitor and receiver***


- Source: Amazon.com

As an alternative to these traditional radio-based devices, the security camera market realized that their technology could fill in the gap created by this limitation. The newest wave of security monitoring devices operated using Internet protocol, the main method of communication through the Internet between devices. This meant that the new products could be accessed over the Internet anywhere in the world. Having access to the baby monitor from anywhere in the world vastly increased the convenience of using these devices, and thus the baby monitor marketplace significantly changed after this. However, as with all Internet enabled devices, this left open the possibility of hacking. Until August 2013, no significant events had occurred that would raise the fears of parents. But this changed that day, in a significant manner.

Inside the 10-month-old baby Emma's room, a stranger was yelling, "Wake up baby. Wake up baby." (Heather Shreck, 2013) After this the man's voice continued screaming at her until the baby woke up. As soon as the parents heard, they ran into the

room. That's when the camera turned towards the father and the man started screaming at him too.

***Pictured: One of Foscam's IP camera models***


- Source: Amazon.com

This was not an isolated incident. During the same month in Houston, Texas, Marc Gilbert was doing the dishes when he heard a strange sound coming from his child's bedroom. He ran into the room only to hear a stranger's voice coming through the IP camera yelling expletives at his daughter. The stranger then turned his attention towards the parents and began swearing and screaming at them too. At this point the father unplugged the camera and attempted to figure out what happened. An especially creepy part of this story was that the stranger had seen the daughter's name written on the wall, and was using it multiple times while swearing at her. Before this incident, the father, Marc Gilbert, had been quoted as saying "We almost couldn't live without it." (Marc Gilbert, 2013) He most assuredly changed his mindset after this incident.

**Double-Edged Sword**

In both of these events, the hacker was able to access the camera based on a flaw pointed out in a security presentation by researchers in the field.The presentation was called *"To watch or to be watched: Turning your surveillance camera against you."* and made by Sergey Shekyan and ArtemHarutyunyan. This research paper, presented as a security warning to the industry members, specifically pointed out a way to hack into the products of a Chinese company called Foscam. Shortly after this research paper was released, a collection of hackers started posting the information on various forums and message boards such as Reddit and 4chan.

In fact, the same researchers showed evidence that by using an online search engine called Shodan, that there were about 100,000 Foscam based IP cameras online that were vulnerable to the same attacks.

The research ended up being a double-edged sword. It gave the company ample warning that they had a massive security risk, yet it appears that Foscam did nothing to prevent it. Only when they were shamed in the media did they start to react.

The security presentation specifically outlined how to hack into and get away with this crime. In the end, the hackers were able to get away with the crime because when these cameras were powered off, the logs of IP addresses were wiped.Thus destroying all evidence of where the hackers came from and how they gained access.

**More Than One Company**

Foscam was not the only industry player to sell IP cameras vulnerable to hacking. In January 2012, thousands of live feeds to IP cameras all over the world were being listed online. Places like a Laundromat in Las Angeles, rooms inside of homes in Korea, office places in Russia, and many more.

The company at the base of these attacks was called TRENDnet. A Torrance, California based company that began selling IP camera products in 2010. This time, roughly 700-1000 live feeds from cameras worldwide were up for display on various websites. By looking at the website data, Katie Notopoulos, a tech writer for The Verge, claims that each feed had possibly 100's or 1000's of viewers. Certainly a terrifying thought considering most of these cameras were placed inside the privacy of people's homes.

***Pictured: Example of TRENDnet IP camera model***

- Source: Amazon.com

The source for these incidents was a hacker going by the name of SomeLuser that ran a blog called Console Cowboys. This hacker posted a long entry about how to attempt and gain access to a specific TRENDnet IP camera. He even posted several screenshots of cameras that he personally hacked. He posted this on January 10th, 2012.

Again, after this was up for display on the Internet, and people realized they could have live access to other peoples' private lives, the post went viral on websites like 4Chan and Reddit. TRENDnet itself first learned of the incident on January 13th, 2012 when a user contacted TRENDnet about the problem. At this point, there were at least already 700 separate TRENDnet IP cameras available on the Internet to be accessed by anyone.TRENDnet was already significantly behind in a battle it didn't even know it was fighting.

Clearly, both of these major players in the IP camera industry weren't the only ones concerned about security vulnerabilities in their products. All IP camera companies were inherently at risk of having their products hacked, how to deal with the prevention of these incidents was of utmost importance to them. More importantly, how to respond to these hacking incidents would determine the future of any of these companies in the IP camera market.

**History of Hacking and Computing**

What is known as the modern personal computer first began proliferating in 1973 with the introduction of the Wang 2200. IBM and many other companies soon followed in the following decade. By the early 1990's, it was common to see a personal computer in most people's houses and dwellings.

The world's first email was sent between two computers sitting in the same room in 1971. Surprisingly, the world's first computer virus, The Creeper, was actually sent out shortly after in the same year! It was created as an experiment at a company called BBN, which was also the same company where the first email was created. Immediately following this was the world's first anti-virus software called The Reaper.

The computer industry, from its very roots has always been a mixed blessing. Computers have vastly changed the way the world operates, but it has also led to the

potential exposing of incredibly important information, which can be accessed from anywhere in the world.

In the early 1980's, what we now know as the Internet was started as a large collaboration between governments and individuals around the world. The world's first web browser was initially titledWorldWideWeb and later changed to Nexus. It was created in 1991. In the same year, the introduction of the first webcam was made.

At its very beginning, the webcam was involved with security in mind. This was not in the traditional sense of the word, however. The webcam was invented to find out who was leaving the only pot of coffee empty in the computer lab at Cambridge University. The students and professors there created a program called 'XCoffee' using a spare camera and a computer in the lab. It allowed anyone with access to the program to put a small real-time video of the coffee pot in the corner of the user's screen. After web browsers became commonplace in 1993, the same users modified the program to be accessed via the web. As the spread of the Internet ensued, the XCoffee webcam ended up having millions of viewers worldwide, simply for the novelty of a remotely accessed camera.

In 1984, what some argue as the World's first B2C transaction occurred in the United Kingdom, between a local grocery store and a 72-year-old grandmother named Jane Snowball. The late 1990's led to the beginning of the e-commerce phase of computing, with Amazon.com and Alibaba.com both being started during this period. (wikipedia) The trend in performing business transactions online continued at a staggering rate. The Boston Consulting Group has stated that by 2016, "the Internet economy will reach $4.2 trillion in the G-20 economies." This would place the Internet's GDP, if it were a country, at number five in the world!

**Cybercrime**

With the advance of a new industry, crime was certain to follow. Cybercrime has been defined as:

> *"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". (1)*
>
> *- Dr. DebaratiHalder and Dr. K. Jaishankar (2011)*

This new industry opened up a virtual playground to the organized crime of the world and allowed them to move into areas previously never even considered. Perhaps one of the better examples of this is the Russian Business Network, which was registered as an official site in 2006. What began as a legal form of business, hosting legitimate companies and legal activities, soon began to make way to one of the largest online criminal networks in existence. An example of one of its more famous activities was called Rock Phish. This scam involved tricking banking customers into giving up their personal financial information. The scam netted over $150 million USD according to VeriSign, an Internet security company.

The vast levels of anonymity and lack of jurisdictional laws has allowed massive amounts of money to be stolen, proliferated, scammed, and embezzled. Norton, a well-established Internet security has estimated annual cybercrime costs “the global economy $338 billion a year, overtaking a still a lucrative trade in the underground drugs market.” (Zack Whittaker, 2011)

Yet, conducting cybercrime solely for the purpose of financial gain is only one facet of the problem. Many cybercriminals simply want to make their mark online by

hacking highly defended websites and to cause disruption in the online and real world. A pertinent example of this is when the Associated Press' Twitter account was hacked in the USA. The hacker posted a fictional tweet stating that an attack occurred in the White House and hurt President Obama. This seemingly minor tweet resulted in a brief dip of 130 points on the Dow Jones Industrial Average. In addition, it resulted in a loss of $136 billion from the S&P 500. Although only a temporary removal of value, the profoundness of the negative result surely left its mark on the Internet security world.

Hacking is no longer just a monetary game. Every industry that is significantly involved in the World Wide Web, which is fast approaching every single one, needs to be prepared for hacking incidents. Assuming that an organization's web security levels are unbreakable is a vast mistake to be made. Every organization with an online presence needs to be prepared for a hacking event. Not doing this simple defensive maneuver can cost an organization dearly, whether it is reputation, embarrassment, or data loss, they all will certainly involve losing money in the long run.

**Industry Response**

Foscam had taken a laissez-faire approach to responding to the incident surrounding the hacking of its cameras. Instead of proactively approaching media and news organizations with damage control methods, it instead simply wrote a blurb on its website initially stating that they were updating the firmware to solve the problem in the future. In fact, the only information even referencing the fact that over 100,000 of its IP cameras were vulnerable to hacking is its 'Company News' section, of which the entirety of the webpage consists of the information located in Appendix 1 and 2. The only information even referring to the major hacking incidents is the sentence stating, "recently, Foscam has received some feedback from our customers and media about camera security problems." **(Appendix 1)**In addition to this, the website states a number of methods to prevent the camera from being hacked. At no point does the website indicate that it was at fault nor apologize for having several thousand customers have their personal lives invaded as a result of its products. One of the major solutions was to

update the device's firmware by directly downloading the software update from the company website.

Certainly this company would benefit from the use of a public relations strategy. In this day and age of two-way communication between large corporations and their customers, especially those in the high-tech industry, this low level of communication is simply unacceptable.

TRENDnet's repercussions and response underwent a different path. It first learned of the hacking scandal three days after the initial intrusions.By January 30th, TRENDnet had released a critical update to the firmware. By installing this update, the IP camera users would be able to prevent the previous type of hacking from occurring. However, the main caveat with this is that of informing the customers. The company was limited in its response and capability of reaching its customers. Most users did not sign up to receive email from the company, as such TRENDnet had no direct way of contacting them. It essentially was limited to the amount of news coverage and posting on the company website. This was the same inherent problem that Foscam faced with its software update.

Another aspect to consider is the amount of media coverage that occurred once the mainstream media learned that baby monitors were being hacked. The negativity around such a thing occurring made for good news stories. This was also in between the period of the hacking and the solution being provided. Twenty days after the incident occurred, the amount of major news sources wanting to report on the incident was much lower, thus the opportunity to provide the solution to customers viewing this initial wave of news coverage was lost. The point can be argued that news media tend to over report negative news and underreport positive occurrences.

Again, it can be seen that TRENDnet would have significantly benefited by having a public relations plan in place after such a hacking scandal. Both of these high-tech companies treated the problem as a purely technical one. Their actions did not

demonstrate that they actually cared about consumers. They simply spent all of their resources working out a solution, which although appropriate, did not consider the human aspect of the business. Their lack of empathy and reacting in a very technical matter to a very human problem certainly cost them significant business in the long run.

**Going Forward**

Since the initial incidents, there has been a lot of activity and interest from the Federal Trade Commission in the United States into these affairs. Of note is that no information could be found about Foscam relating to the FTC. This is most likely because Foscam is a China based company and out of reach of the jurisdiction of the FTC.TRENDnet on the other hand, is based in the United States.

On February 7th, 2014, the FTC issued a press release regarding this company. They had examined the case of the TRENDnet hacking incidents and came up with a series of punishments. The FTC alleged that TRENDnet was marketing its IP cameras as being secure, yet because of the extreme ease to hack these cameras, this was concluded to be a misrepresenting statement.

The punishments included several different sentences. Firstly, the company had to immediately stop misrepresenting the security of the cameras and to stop stating how the information captured from the cameras is secure. They were also required to setup a "comprehensive information security program designed to address security risks that could result in unauthorized access to or use of the company's devices." Another punishment was that TRENDnet had to attain third-party assessments of this security program every other year for 20 years into the future. Lastly, it required the company to contact every customer to notify them of the vulnerabilities as well as offer them free technical support for the next two years. It is interesting to see that they did not actually have to pay any fines, which would likely have been quite substantial. This is probably due to their quick response when first finding out about the hacking.

All of these punishments set TRENDnet back quite a bit in terms of both time and resources. Foscam may face similar consequences in the future if similar incidents happen to them as well. The ease with which people were able to hack into these IP cameras is a fundamental problem of the industry and is not an easy fix. The companies have to prepare defenses, employ better encryption, and have a way to update their customers' firmware if they want to prevent these incidents from reoccurring. The problem is, all of these actions are incredibly expensive and these companies sell products in a 'lower cost, the better' price environment.

The companies involved in this industry are faced with ever advancing hackers, a lot of whom have the 'put a penny on the railroad tracks' attitude towards the Internet. For these kinds of hackers, it doesn't matter that there is no monetary gain at the end. If the possibility of looking into someone else's private home exists, people will want to see it. How to battle these future incidents should be at the forefront of every IP camera company leader's mind.

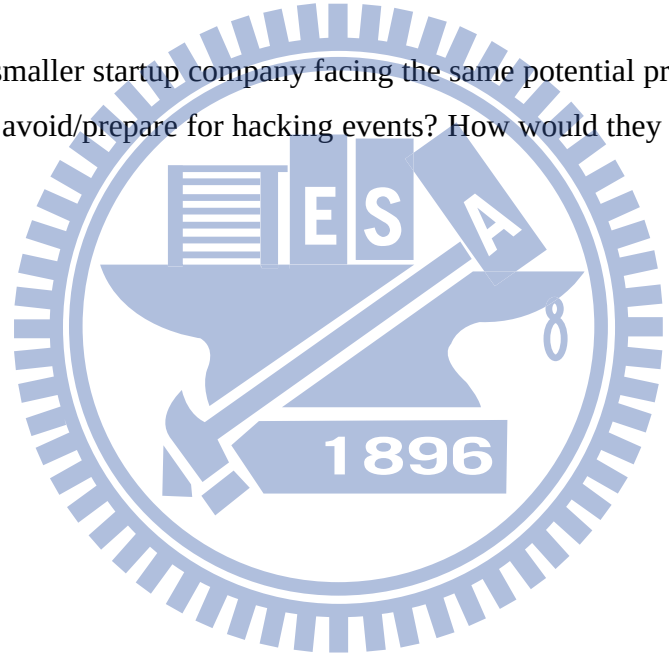
**Discussion Questions**

1. If you were the Foscam CEO at the time of the first incident, what steps would you have taken immediately after finding out about the hacking?

2. What, if anything, should Foscam have done before this incident in order to prepare for hacking events?

3. How would you react as a competitor of Foscam? Would this be good for your company or bad?

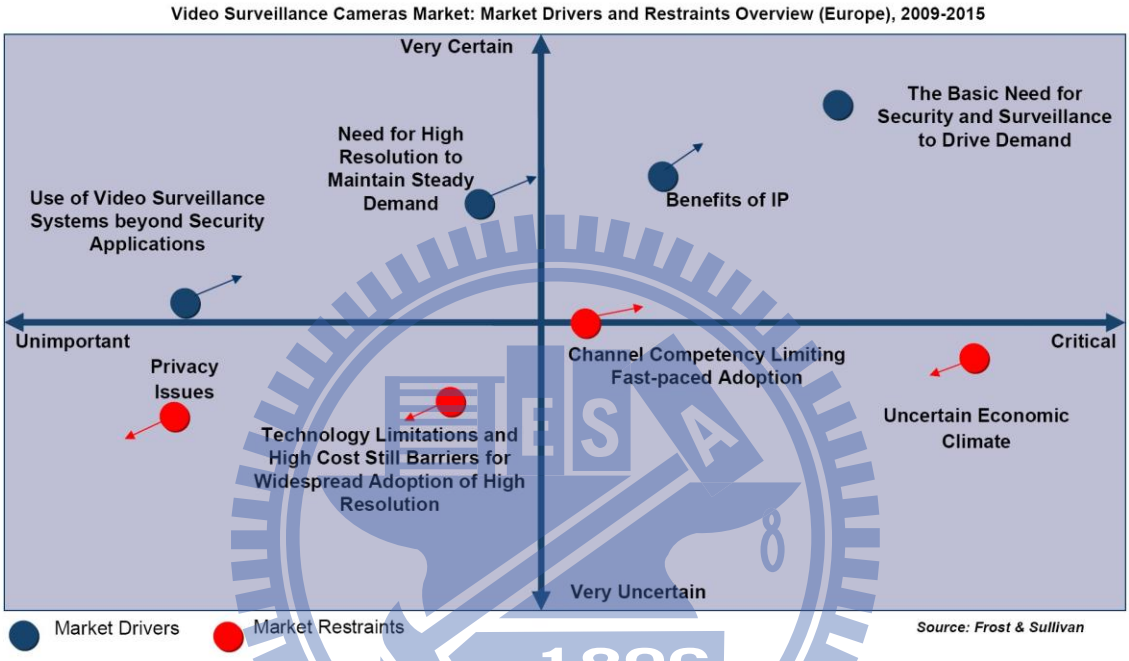
4. As a CEO of a smaller startup company facing the same potential problems, what steps would you take to avoid/prepare for hacking events? How would they differ from being a large company?



**IP Camera Industry Related Information**

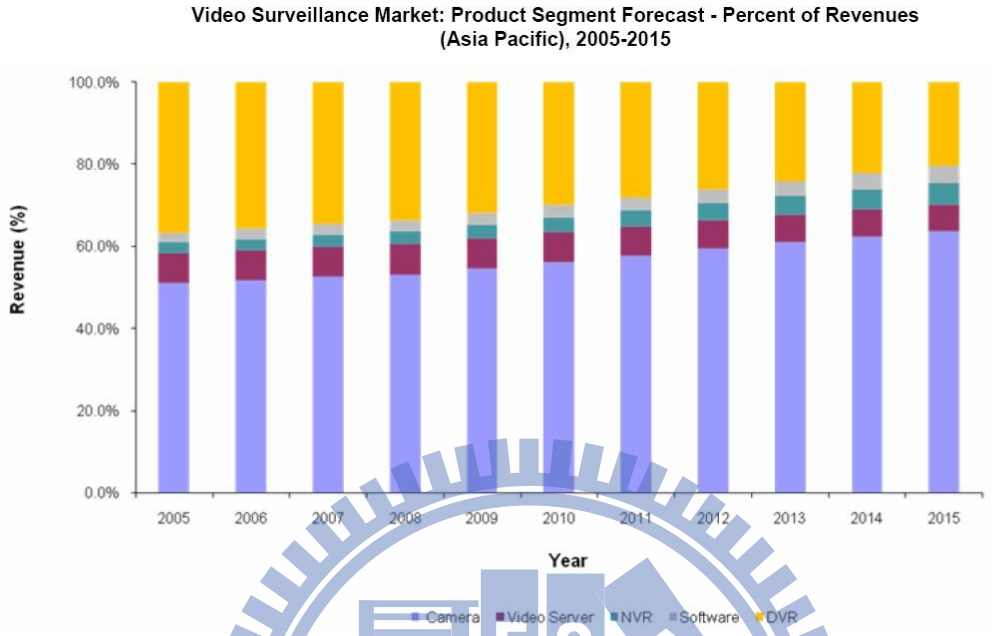
1. Global IP Video Surveillance market to grow at a CAGR of 24.89 percent over the period 2013-2018

2. Video Surveillance Cameras Market Overview




3. Though analog still accounts for a majority of sales, Frost & Sullivan expects revenues for IP-based technology in the European video surveillance camera market to increase from $765 million in 2009 to nearly $959 million by 2015.

4. Pictured: Video Surveillance Market Forecast




*Note: All figures are rounded; the base year is 2008. Source: Frost & Sullivan*

5. Pictured: Market Drivers for IP cameras

**Total Internet Protocol (IP) Surveillance Market: Market Drivers Ranked in Order of Impact (World), 2006-2012**

| Rank | Driver | 1-2 Years | 3-4 Years | 5-7 Years |
|---|---|---|---|---|
| 1 | Need for remote accessibility of real time data expands the market for IP surveillance solutions | Very high | High | High |
| 2 | The drawbacks of existing systems instigates the need for IP surveillance | Very High | High | Medium |
| 3 | Flexibility of the IP surveillance systems stimulating the demand for this technology | High | High | Very high |
| 4 | Efficiency of IP surveillance systems creating demand for this technology | High | High | Very high |
| 5 | Reduced cost factors driving the market for IP surveillance solutions | High | High | Medium |
| 6 | Reduction of risk exposure due to customized solution offering upholds the market revenues for IP surveillance technology | Medium | High | Very High |
| 7 | Decreasing digital technology prices encouraging the end users to adopt IP surveillance technology | Low | Medium | High |

*Source: Frost & Sullivan*

6. Between 2010 and 2012, TRENDnet's "Secureview" line made $19 million in revenue, accounting for 10 percent of the company's total revenue during that time period.

7. Pictured: Foscam Sales Revenue 2008-2012

# V. Action-Plan for Hacking Event of IP Camera Company

## 5.1 Optional Actions

The following section is the work of the author and his opinions on how previous work in the public relations research field can be modified to create a plan of action for companies in the IP camera industry to plan for potential hacking events.

Firstly, we can look at the chart contained on page 18 referring to the different costs associated with different types of media available for use by companies in public relations. By following the principles of Grunig and his beliefs that two-way asymmetrical communication systems are optimum, we should be choosing options that are located on the far right side of this chart.

Amongst these options are open corporate social media site, Twitter accounts, interactive online community contributions, open sourcing, open API's, wiki/open 3rd party editable information and use of content sharing sites. As the reader goes farther to the right, the time cost increases, but incidentally so does the level of trust.

Keeping in mind the intricacies of the IP camera industry, we can see from Foscam and TRENDnet's websites that they already employ an interactive online community. The caveat with this is that although the communities themselves appear to be quite active, the response rate of the companies does not seem to be quite high.

Firstly, we can take a look at what tools would be appropriate for an action-list. The researcher would recommend that the following tools be selected from the aforementioned options:

- *Twitter/Facebook accounts*
    - These are free accounts that provide a simple and effective way to reach

the masses. Users simply need to follow the account and can gain an insight into whatever the company wants to tell. Simultaneously, the companies can gain instant feedback from consumers when they have problems. These accounts usually require an active monitoring by a person in charge of media.

- *Interactive online community*
    - These forums can provide discussion and problem solving in the customer community itself. It also allows companies to monitor what people are thinking about the brand, problems, and any other occurrences. These forums do require active moderating, and if not consistently responded to in an appropriate timing, can actually hurt the image of a company. A positive use would be to implement a ranking system where the users can vote for each post. Such a system would 'automatically' rank customers interests by priority, and thus make it easier for a company to respond quickly.
- *Open source/Open API's*
    - Utilizing this strategy might be an extremely effective way for a company to cheaply and efficiently solve the problem of whatever hacking problem it is encountering. By opening up the system to the public, without revealing too key information, the high-tech crowd might be inclined to improve the software to make it more secure or to function better. If a hacking event were to occur, some customers might jump at the chance/challenge of stopping the hacker's exploit. This would be for the challenge and for the reason of securing their own IP camera. The main problem with this approach is that companies would have to change the essence of their firmware and software to allow it to be modified. They would also have to determine how much software they would let the public change on its own, a balance of security and power.

The next step is to create the action plan. The four-stage action plan set out by Alfonso Gonzalez-Herrero and Suzanne Smith is used as the basis and modified

according to the author's thoughts. This paper presents a much more concise plan than the plan it builds on as it can be more effective as it is specific to a certain industry. The four main titles shall be used again. This includes issues management, planning-prevention, crisis, and post-crisis.

## 5.2 Revised Action List

### 5.2.1Issues Management

1. Assign resources – human and economic – to organize the entirety of the action plan, be sure to assign a crisis management leader to be in charge of the situation when it happens
2. Establish the budget and constraints
3. Draw a full map of online influencers showing issues of interest or concern.
4. Establish an efficient online monitoring alert system that includes monitoring of websites, blogs, newsgroups, etc.
5. Draw up a list of potential issues that may occur and rate them according to their probability of occurrence and level of damage to the organization
6. Draw up guidelines on the approach, tone, and language that is appropriate for dialogue in a dynamic, online environment. This will be quite different from the more formal and distant corporate tone and language used in traditional communications.
7. Set-up proper media tools for use in communicating with the public such as Twitter, Facebook, interactive online community – Assign enough manpower to be able to monitor and respond to these media without significant delays

### 5.2.2 Planning-Prevention

1. Create method of updating firmware of customers IP cameras – either through a mandatory mail list, a heavily secured backdoor, or another method
2. Update e-mailing lists and contact databases – keep a centralized database with a backup, that can be accessed by multiple authorities and access points

3. Draft guidelines on how to respond quickly to news of hacking incidents
4. Check whether the regular media monitoring service is fast enough to follow the crisis, especially for online media outlets.
5. Pre-create webpages to immediately turn on-line in case of hacking – these pages should contain all possible information about hacking, what can be done, and who to contact
6. Evaluate your in-house capabilities to develop graphic, video, and audio files that could be quickly distributed online, whether they are simple digital pictures or more elaborate podcasts. Purchase the necessary equipment or think about outsourcing these services.
7. Consider whether you need your traditional PR firm to do online PR or you need to hire a separate PR firm or partner that specializes in online PR.
8. Search for and attain potential allies on the internet that can assist in times of crisis – popular bloggers, writers, or high-tech enthusiasts having an active input to the team can grant very valuable 3rd party support
9. Test the online crisis plan.

.

**5.2.3 Crisis**

1. Have designated crisis management leader take control and know who is reporting to him/her
2. Ensure your mainstream media and online monitoring services are aware of the crisis situation and that they report electronically all outcomes as they appear.
3. Use search engine optimization to make the company's web site appear at the top of a search.
4. Launch the previously hidden webpage and update the information as fast as possible
5. Use links to reputable third-party endorsements or to web sites that have favorably covered the issue.
6. Link to bloggers or other friendly influential internet presences previously established

7. Use the web for further information or instructions to consumers and the audience (e.g., In the case of a product recall, etc.). Make sure announcements are clearly seen from the home page.
8. Use any tool available (chat rooms, forums, social media) to ascertain what the audience's problems are and what can be done to solve them
9. Get CEOs to use the Internet to personally address stakeholders, something few of them do, according to Stock (2003).

### 5.2.4 Post-Crisis

1. Continue tracking the issue by monitoring blogs, online media, etc. during the months – and even years – to come.
2. Thank those who helped the company during the crisis. From an online point of view, this could include 'thank you' e-mail messages or a 'thank you' message on the company's web site.
3. Have the company's social media relations not avoid the issue of the hacking scandal – it is important to maintain an honest and open feel in order to regain the audience's trust
4. Define the strategies and tactics at play to rebuild the company's reputation: from in-depth analysis of Internet content and opinion leaders, to online chats with the most active bloggers.
5. Evaluate what happened and how the organization responded, so that the crisis plan and all the online related measures could be properly adapted.

## VI.Conclusion

The researcher started this project with the goal of being able to assist those in the IP camera industry in preparing for hacking scandals. It is the researcher's belief that given the high-risk nature of hacking scandals and the voyeuristic temptations offered by having IP cameras available on the web that there will most likely be many more hacking scandals in the future in this industry.

The researcher hopes that the modified guidelines set out in the research will be able to assist companies and stakeholders in the future as they plan and prepare for such situations. This plan is unproven in practice, but is based upon the work of previous researchers in the field of public relations. It also takes into account the researcher's personal experience in the industry and the problems he has encountered.

It is likely that there will be hacking scandals in the future in the IP camera industry and it is imperative that companies prepare for this occurrence. There are a lot of factors to consider and many different ways to ward off the chances of this happening. However, by employing the tools outlined in the action plan above, not only will a company be adequately prepared for a hacking event, but they will also open up their doors to the benefits of a two-way symmetrical communication environment. It is Grunig's belief as well as the researcher that this method of public relations is superior to the others in the four models. By interacting with the stakeholders on an even basis, trust is garnered in a company; this is something that is highly appreciated in the modern age.

This extra trust will likely lead to increased sales and a great reputation for the company's brand. Having a proper public relations plan in action will help any company in any industry. In today's environment, having minimal or no public relations at all is a costly mistake to make, and will lead to trouble for the company in the future. Transparency and preparedness are the key in planning for a hacking event in the IP camera industry.

## VII. References

1) Halder, D., &Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

2) Waxman, Olivia. "Stranger Hacks Into Baby Monitor and Screams at Child". *Time*. Time Inc. Retrieved 30 April 2014.

3) Sison, M. (2009). Theoretical Contexts. In J. Chia and G. Synott, (eds.), *An Introduction to Public Relations: From Theory to Practice.* (pp.54-89). South Melbourne: Oxford University Press.

4) Sterling, Bruce (1993). "Part 2(d)". The Hacker Crackdown. McLean, Virginia: IndyPublish.com. p. 61. ISBN 1-4043-0641-2.

5) Taylor, Paul A. (1999). Hackers: Crime in the Digital Sublime. Routledge. ISBN 978-0-415-18072-6.

6) Franklin, Bob; Hogan, Mike; Langley, Quentin; Mosdell, Nick; Pill, Elliot (2009). "Target audience".Key concepts in public relations. SAGE. p. 227. ISBN 978-1-4129-2318-7.

7) Shrivastava, P. Mitroff, I.I., Miller, D. and A. Miglani, " Understanding industrial crises".Journal of Management Studies, 1988, 25, 4, 285-304.

8) ASIS International, "Organizational Resilience: Security, Preparedness, and Continuity Management Systems-Requirements with Guidance for Use, ASIS SPC.1-2009, American National Standard", 2009

9) Natasha Tobin, (2005), "Can the professionalisation of the UK public relations industry make it more trustworthy?", Journal of Communication Management, Vol. 9 Iss: 1 pp. 56 – 64

10) Cutlip, Scott (1994), The Unseen Power: Public Relations: A History, Lawrence Erlbaum Associates, ISBN 0-8058-1464-7

11) James E. Grunig (2000) Collectivism, Collaboration, and Societal Corporatism as Core Professional Values in Public Relations, Journal of Public Relations Research, 12:1, 23-48, DOI: 10.1207/S1532754XJPRR1201_3

12) K. Sriramesh ,Yungwook Kim &Mioko Takasaki (1999) Public Relations in Three Asian Cultures: An Analysis, Journal of Public Relations Research, 11:4, 271-292, DOI: 10.1207/s1532754xjprr1104_01

13) Grunig, J E. "Paradigms of global public relations in an age of digitalisation." Prism 6.2 (2009):1.

14) Basso, J, andBasso. "How public relations professionals are managing the potential for sabotage, rumors, and misinformation disseminated via the Internet by computer hackers." IEEE Transactions on Professional Communication 40.1 (1997):28-33.

15) Alfonso, González-Herrero, SmithAlfonso, andSuzanne. "Crisis Communications Management on the Web: How Internet-Based Technologies are Changing the Way Public Relations Professionals Handle Business Crises." Journal of contingencies and crisis management 16.3 (2008):143-153.

16) J.E Grunig, Excellence in Public Relations and Communication Management, Lawrence Erlbaum Associates, Hillsdale, NJ (1992)

17) R Heath, G.M Vasquez, Rhetoric as the Basis for Socially Responsible Public

Relationspaper delivered to the International Communication Association's national conference, Chicago, IL (August 1995)

18) R Pearson, Business Ethics as Communication Ethics: Public Relations Practice and the Idea of Dialogue, C Botan, V Hazleton Jr. (Eds.), Public Relations Theory, Lawrence Erlbaum Associates, Hillsdale, NJ (1989)

19) An Internet Primer for Public Relations, "For excellent introductory discussions of how the WWW works," see Public Relations Quarterly, 40 (3) (Fall 1995), pp. 27–32

20) G.M Santoro, "The Internet: An Overview," Communication Education, 43 (2) (April 1994), pp. 73–86

21) P.H Lewis, "Trying to Find Gold With the Internet." New York Times (3 January 1995)

22) M.A Johnson. "Public Relations and Technology: Practitioner Perspectives." Journal of Public Relations Research, 9 (3) (1997), pp. 213–236

23) Levine, R. (2009). The cluetrain manifesto (10th anniversary ed.). New York: Basic Books.

24) Grunig, J. E. (2009). Paradigms of global public relations in an age of digitalization.PRism, 6(2), 1-19, Retrieved March 15, 2014, from http://www.prismjournal.org

25)Sledzik, B. (n.d.). The '4 Models' of public relations practice: How far have you evolved?.ToughSledding. Retrieved March 3, 2014, from http://toughsledding.wordpress.com/2008/08/10/the-4-models-of-public-relations-practice-how-far-have-you-evolved/

26) Wang, K. (n.d.). Example: I'd Rather Go Naked Than Wear Fur Campaign. PETA PR

Exhibition. Retrieved June 3, 2014, from http://petapr11.wordpress.com/2009/04/27/example-2-id-rather-go-naked-than-wear-fur-campaign/

27) Stevenson, S. (n.d.). Stevenson, Sarah: Communication models and uses within the working practices of PR. PR Current Issues Future Directions. Retrieved April 29, 2014, from http://prwisdom.wordpress.com/communication-models-and-uses-within-pr-working-practices-sarah-stevenson/

28)TRUTH Campaign/Public Information Model. (n.d.). PR Group 13s Blog. Retrieved May 10, 2014, from http://prgroup13.wordpress.com/2009/04/29/truth-campaignpublic-information-model/

29) Phillips, D. (2009, January 9). LeverWealth. : A Grunigian view of modern PR. Retrieved May 20, 2014, from http://leverwealth.blogspot.com/2009/01/grunigian-view-of-modern-pr.html?disqus_reply=5552359#comment-5552359

30) Gonzalez-Herrero, A., & Smith, S., (2008). Crisis Communications Management On The Web: How Internet-Based Technologies Are Changing The Way Public Relations Professionals Handle Business Crises. Journal of Contingencies and Crisis Management, 16(3), 143-153.

31) Gonza´lez-Herrero, A. (1994), A Model in Crisis Communications Management. Master's Thesis, University Microfilms International, Michigan. Limited circulation.

32) Gonza´lez-Herrero, A. and Pratt, C. (1995), 'How to Manage a Crisis Before – or Whenever – It Hits', Public Relations Quarterly, Volume 40, Number 1, pp. 25–29.

33) Gonza´lez-Herrero, A. and Pratt, C.B. (1996), 'An Integrated Symmetrical Model for Crisis-Communication Management', Journal of Public Relations Research, Volume 8,

Number 2, pp. 79–105.

34) Waxman, O. (August, 2013). Stranger Hacks Into Baby Monitor and Screams at Child. Time. Retrieved May 29, 2014, from http://time.com/79170/stranger-hacks-into-baby-monitor-and-screams-at-child/

35) Hill, K. (2013, August). How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old. Forbes. Retrieved March 30, 2014, from http://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/

36) Willey, J. (2013, August). Hacker targets Houston family's baby monitor, father catches him saying disturbing things to sleeping toddler. ABC13 Houston. Retrieved March 30, 2014, from http://abc13.com/archive/9201651/

37) Shekyan, S., Harutyunyan, A. (Directors) (2013, April 11). To watch or to be watched: Turning your surveillance camera against you. Hack In The Box. Lecture conducted in Amsterdam.

38) Kerr, D. (n.d.). FTC and TrendNet settle claim over hacked security cameras - CNET. CNET. Retrieved May 15, 2014, from http://www.cnet.com/news/ftc-and-trendnet-settle-claim-over-hacked-security-cameras/

39) Notopoulos, K. (n.d.). Somebody's watching: how a simple exploit lets strangers tap into private security cameras. The Verge. Retrieved April 28, 2014, from http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan

40) consolecowboys: Trendnet Cameras - I always feel like somebody's watching me.. (n.d.). consolecowboys: Trendnet Cameras - I always feel like somebody's watching me.. Retrieved May 10, 2014, from http://console-cowboys.blogspot.tw/2012/01/trendnet-cameras-i-always-feel-like.html

41) Wang2200.org. (n.d.). Wang 2200. Retrieved May 10, 2014, from http://www.wang2200.org/

42) Meltzer, T., & Phillips, S. (2009, October 23). From the first email to the first YouTube video: a definitive internet history. The Guardian. Retrieved June 4, 2014, from http://www.theguardian.com/technology/2009/oct/23/internet-history

43) The Internet Economy in the G-20: A Country-by-Country Interactive. (n.d.). www.bcgperspectives.com. Retrieved June 4, 2014, from https://www.bcgperspectives.com/content/interactive/digital_economy_technology_software_internet_economy_g20_country_by_country_interactive/

44) A walk on the dark side. (2007, August 30). The Economist. Retrieved May 15, 2014, from http://www.economist.com/node/9723768

45) Whittaker, Z. (n.d.). Cybercrime costs $338bn to global economy; More lucrative than drugs trade | ZDNet. ZDNet. Retrieved May 20, 2014, from http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503

46) Security Camera Vendor TRENDnet Settles With FTC Over Lax Internet Security. (n.d.). Channelnomics RSS. Retrieved May 19, 2014, from http://channelnomics.com/2013/09/05/security-camera-vendor-trendnet-settles-ftc-lax-internet-security/#.U4xmEy_6q5s

47) 2018 IP Video Surveillance Industry: Global Trend, Size and Growth Analysis Report. (n.d.). Academia.edu. Retrieved May 11, 2014, from http://www.academia.edu/5461943/2018_IP_Video_Surveillance_Industry_Global_Trend_Size_and_Growth_Analysis_Report

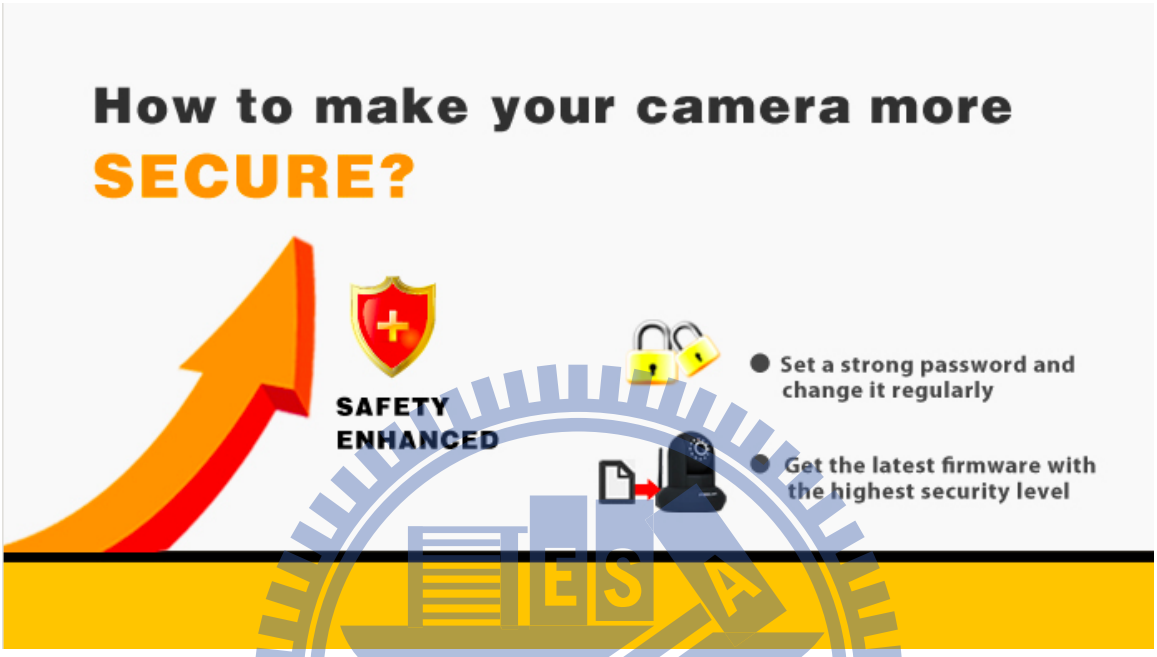
48) Report: IP makes gains on analog market in Europe. (n.d.). SecurityInfoWatch.com. Retrieved May 20, 2014, from http://www.securityinfowatch.com/news/10499009/report-ip-makes-gains-on-analog-market-in-europe

49) Wyatt, Edward. "F.T.C. Says Webcam's Flaw Put Users' Lives on Display".New York Times. Retrieved 1 April 2014.

50) Foscam-Ukraine Corporate Website. (n.d.). Foscam. Retrieved May 20, 2014, from http://foscam-ukraine.com

## VIII. Appendixes

1.




- Source:foscam.com

2. Webpage of Foscam's 'News' Section

**Some Security Tips to Make Your Camera Safer**

Recently, Foscam has received some feedback from our customers and media about camera security problems. Foscam takes security very seriously and has a dedicated team who is constantly engaged with network professionals around the world to carry out security testing on our cameras. Our team carried out detailed research on this issue and found the reasons are:

a. Some of our customers are still using the default username and password.
b. The username and password is too simple and easy to crack.
c. Some of the cameras are still using the old firmware and have not been upgraded to

the latest version.

To ensure the security of your camera and prevent various types of hacking and unauthorized access, Foscam strongly recommends our customers to safeguard their privacy by taking the following security precautions.

1）Always change the default username and/or password as soon as you setup your camera. Input a username and/or password that is at least 8 – 10 characters or longer. Try to use a combination of lower-case and upper-case letters as well as numbers and special characters.

2) Make sure your camera has the latest security firmware installed for your specific camera model. The latest firmware for Foscam cameras utilizes protection against various types of online hacking and unauthorized access.

Step1: Go to our official download center http://www.foscam.com/down3.aspx
Step2:.Check the model and current firmware version of your camera carefully, and then choose the right firmware to download.
Step3: Unzip the firmware RAR file. There will be firmware files and upgrade guidance. Please follow the guidance carefully to upgrade the firmware.

3) Change your default port to a port in the 8100 or greater range. Hackers often target default ports and you do not want to make yourself an easy target. By using a non-standard port it will make it more difficult for hackers to find your camera.

4) Check the logs of your Foscam cameras often. Foscam cameras have embedded logs which allow you to see exactly which IP addresses are accessing the camera. You will be able to tell if an outsider has gained access to your camera.

5) Make sure your Internet router or modem is secure (ie, change the default password and install updates), since this is how the device will connect to the Internet.