Enterprise's Online Trust Crisis Management: A Life Cycle View

Yitang Zeng[1] and Chunhui Tan[2,*]

[1] School of Information Management, Wuhan University, Wuhan, China
ztqingwen@163.com
[2] School of Information Management, Central China Normal University, Wuhan, China
tanadan@mail.ccnu.edu.cn

Abstract. Online trust is the vital mechanism for the development of e-commerce, and the significance of online trust has become a consensus. Undeniably, an obscure message may be magnified indefinitely and evolve into the enterprise's online trust crisis, which will affect the image of the enterprise, threaten the survival and development of the enterprise, or make the enterprise into a doomed situation that can never be recovered. We study the development phases of enterprise's online trust crisis life cycle, and then put forward framework of enterprise's online trust crisis management strategies based on the characteristics of online trust crisis life cycle, which may be provide some theoretical supports for enterprise's online trust crisis management.

Keywords: Online trust, online trust crisis, online trust crisis management.

1 Introduction

1.1 Background

After more than ten years of fast development, the Internet has brought reforms on people's life styles, modes of information transmission, enterprise's managing ways, and ideas of government administration. According to the "Internet World Stats" [1], by the end of June 2012, about 26% of the World's population has Internet access, which represents 566.4% more than in year 2000. Regions like North America and Europe are well above those figures, with 78.6% and 63.2% of the population having online access respectively. The "33th statistical report on the Internet Development in China" [2] showed that the number of Chinese Internet users have reached 618 million, and Internet penetration rate has raised to 39.9% by the end of 2013.The scale of e-commerce has grown substantially over the past years. Global business-to-consumer e-commerce sales will pass the 1 trillion euro mark by 2013, according to a new report by the Interactive Media in Retail Group (IMRG) [3], a U.K. online retail trade organization. The e-commerce of China has a rapid growing; the total value of E-commerce in China was 5.6 trillion Yuan (about 675 million euro) in the first three quarters of 2012, which grew 25% from the same time of 2011 [4].

---

[*] Corresponding author.

Trust is the currency of all commerce. In traditional commerce, the trust is based such things as societal laws and customs, and on the intuition people tend to develop about each other during interpersonal interactions. As for Internet-based commerce, owing to lacking of the personal relationship, trust becomes even more important. Whether for the traditional entity enterprises, or for the emerging virtual enterprises, online trust is the vital mechanism for the development of e-commerce, and the significance of online trust has become a consensus [5-8]. Online trust can affect consumers' intentions to revisit the site and to recommend the site to others. Online trust plays a key role in creating satisfied and expected outcomes in online transaction. Online Trust has been found to be a significant antecedent to customer's willingness to transact with an e-vendor. Online trust serves to mitigate the perceptions of risk, uncertainty and vulnerability that are associated with the disclosure of personal and identifiable information.

The Internet has proven to be a powerful and very popular vehicle for distributing information to millions of individuals. If there were any negative information about one company in the Internet, this information might diffuse broadly in several hours or even in several seconds. The spread of Internet public opinions often plays the role of the catalyst of corporate crisis and the accelerator of dissemination. An obscure message may be magnified indefinitely and evolve into the enterprise's online trust crisis. Like viruses, online trust crises can be mutated, acquiring new and dangerous forms in, for example, social forums like Facebook, or video distribution sites such as YouTube. Once the enterprise's online trust crisis has be happened, the credibility and reputation of the enterprise will be heavily injured, the word-of-mouth and image of the enterprise will be heavily damaged, and the survival and development of the enterprise will be threaten, or make the enterprise into a doomed situation that can never be recovered. Either in China or in other countries, a lot of famous enterprises have met the online trust crises. Some of them fall in trouble and recovered from the crisis through a very long period. However, some of them were not so lucky and directly ended the corporate life cycle.

The objective of this paper is to address the following research questions:

(1) What is the life cycle of online trust crisis diffusion?

(2) What countermeasures can be used in the enterprise' online trust crisis management in the life cycle of enterprise' online trust crisis?

Hopefully, this study will help enterprises to gain some useful suggestions to manage online trust crises.

1.2   Define Online Trust and Online Trust Crisis

Trust as a social phenomenon has been studied in various disciplines and the notion of trust has been examined under various contexts over the years. Many researchers have interpreted it and made a lot of contributions from the perspective of philosophy, psychology, management, and marketing [9-12]. Among definitions, the generalized definition of trust by Rousseau et al. [13] is broadly accepted. In their opinion, "*trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*"(p.395). Based on the

study of trust, researchers widened the definition of trust and applied it to online trust upon Rousseau's definition, Bart et al. [14] emphasize that "online trust includes consumer perceptions of how the site would deliver on expectations, how believable the site's information is, and how much confidence the site commands" (p.140). Corritore et al. [15] define online trust as "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited" (p.740). In our opinion, online trust is a psychological affirmation of common expectations in an online environment of uncertainty that is caused by online principal parts, based on their wishes, participant's characteristics and the environmental factors, e.g. system, technology and third-party certification.

What is a crisis? The viewpoint of Seeger et al. [16] is representative for an organizational setting. They define that crises are "the specific, unexpected, and non-routine events or series of events that create high levels of uncertainty and threat or perceived threat to an organization's high priority goals" (p.235).

Based on the above notions, the enterprise's online trust crisis means that the related information about the irresponsible behaviors or negative events of the enterprise were published, disseminated and diffused via Internet, which will decline dramatically the degree of trust of consumers, suppliers, distributors, social public, government departments, thus create high levels of uncertainty and threat or perceived threat to one enterprise.

2   Review of Literature

The topic for this study cuts across more than one substantive area in the review of the literature. However, its framework is premised on a strong thematic organization based on the online trust and crisis management.

2.1   Online Trust

The literature on online trust is extensive and multi-faceted and online trust has been extensively studied.

Luo [17] examined several key mechanisms that can help increase customers' trust of e-commerce and decrease privacy concerns. These mechanisms include characteristic-based (e.g., community), transaction process-based (e.g., repeated purchases), and institution-based trust production (e.g., digital certificate). Wang and Emurian [18] pointed out that online trust is a difficult task to accomplish because it requires the establishment of trusting relationships in the online world. The study of Gefen et al. [19] showed that trust in online environments is predicated on beliefs in the trustworthiness of a trustee; trustworthiness is composed of three distinct dimensions-- integrity, ability, and benevolence. Integrity is the belief that the online merchant adheres to stated rules or keeps promises. Ability is the belief that the online merchant has the skills and competence to provide good quality products and services. Benevolence is the belief that the online merchant wants to do good to the customer without regard to making a sale. Beldad et al. [20] provided an overview of the available research into the antecedents of trust in both commercial and non-commercial online transactions and services. There are three clusters of antecedents:

customer/client-based, website-based, and company/organization-based antecedents. Benedicktus [21] offered that online trust beliefs vary positively with consensus ratings and trust is higher when ratings trends increase rather than decrease. Bock et al. [22] evaluated the effects of antecedents of online trust in the context of multi-channel retailers at different phases, taking into consideration the moderating effects of product types. With increases in product uncertainty, the effects of word-of-mouth, offline trust, and efficacy of sanctions on online trust are greater for experience products than for search products. Kim and Ahmad [23] offered a framework for modeling the trustworthiness between a content consumer and a content provider in online social media-sharing communities where users have interacted with each other as either a content consumer or a content provider.

2.2   Crisis Management

Many researchers have discussed crisis management.

Heath [24] introduced an integrated management approach in the Crisis Management Shell Structure, which includes decision component, advisory component, operation component and information component, in terms of what the components units do, why they do these activities, and who is involved. Mak et al. [25] presented a novel application of workflow technology to coordinate and disseminate tasks and related information for Crisis Management Support Systems (CMSS). Their research results indicated that the ability of workflow technology to coordinate, monitor, organize and distribute specific tasks and the associated required information in a timely and efficient manner appears to make it an ideal tool for strategic crisis management. Murray and Foster [26] provided the principles of organizing a multidisciplinary group for crisis resource management. Ryzenko and Smolarkiewicz [27] presented analysis of usefulness of space applications in crisis management activities carried out on the national level. According to them, the key to successful crisis management lays in understanding operational needs; integration into common information environment; and standardization of information exchange. The research of Pearson and Sommer [28] showed that through crisis management planning and preparation, organizational leaders do what they can to make timely decisions based on the best facts that they can gather. Speakman and Sharpley [29] proposed an alternative, chaos theory-based approach to crisis management. The elements of chaos theory include edge of chaos, the butterfly effect, bifurcation and cosmology, self-organization, strange attractors and the lock-in effect. Sardouk et al. [30] proposed a crisis management approach based on wireless sensor networks, which overcomes the problems encountered by the base stations and insures relevant, rich and real-time information about events.

From the previous survey, none of these previous articles focused on the enterprise online trust crisis management. Online trust crisis managing strategies have been substantially altered comparing with the traditional crisis management.

3   The Life Cycle Model of Enterprise's Online Trust Crisis

There is a life cycle for the development of everything in the world. The life cycle concept is originally used to describe a period of one generation of organism in a biological system [31]. Since 1960s the theory of life cycle was raised, the concept of

life cycle is applied widely, especially in the fields of politics, economy, environment, technology, and society. In essence, the term life cycle can be popularly understood as a period "from Cradle to Grave", or from its birth to its end. This also applies to the enterprise's online trust crisis. Similarly, the theory of life cycle can be used to describe the stage of development of enterprise's online trust crisis.

Based on the change of individuals' attention, we investigate the stage of development of enterprise's online trust crisis from the perspective of time series, then the whole online trust crisis life cycle can be divided into four phases (see Figure 1): incubation phase, outbreak phase, diffusion phase and decline phase.
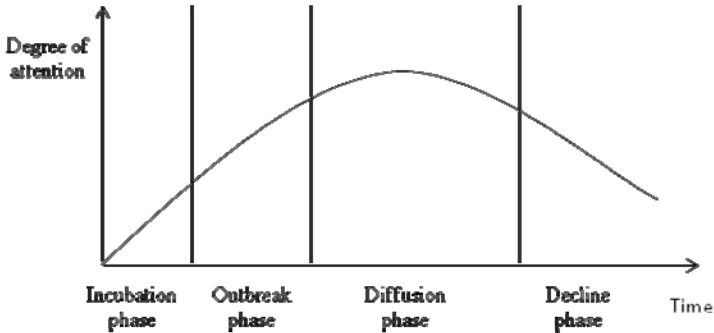

Fig. 1. The life cycle of online trust crisis

There are different characteristics and symptoms in the different stages of enterprise's online trust crisis life cycle. And these characteristics play an important role in enterprise's online trust crisis management. The characteristics of each stage of enterprise's online trust crisis life cycle are shown in Table 1.

3.1   Incubation Phase

The incubation phase includes the period from the appearing of signs of enterprise's online trust crisis to the perceived loss caused by online trust crisis. In this phase, the online trust crisis has not yet broken out; the degree of attention is low. The number of individuals involved is little, network issues are dispersed, the information of online trust crisis is relatively hidden, and the sphere of influence of online trust crisis is small. However, the signs of online trust crisis begin to appear, for example, the sporadic appearance of report on the enterprise adverse events, the sporadic negative comments against the enterprise. If these signs could be taken seriously and handled properly, then the online trust crisis will be nipped in the bud or the damages will minimize to a low degree.

3.2   Outbreak Phase

The outbreak of enterprise's online trust crisis is triggered with potential predisposing factors. There are two sources for enterprise's online trust crisis: one is internal incentive; the other is external incentive [32]. As internal incentive, the corporate

itself produces negative events, such as error of strategies, unfavorable events of functions or deviation of implementation. These will cause the enterprise's online trust crisis, when these negative events are communicated and diffused with Internet news, BBS, blogs and podcasts, RSSs, SNSs, IM, or micro-blogs, just to give some examples of potential channels for the bad news. As external incentive, the negative events usually relate with production and operation. The trust crisis event of the enterprise is reported by Internet news media. The unfavorable remarks on the enterprise are then further released by individuals with social media. The evaluations and reports on the enterprise's crises may also published by other third parties. The adverse information on the enterprise might be published maliciously by competitors. These all will lead to the enterprise's online trust crisis, which is communicated and diffused with network channels.

Table 1. The characteristics of each stage of enterprise's online trust crisis life cycle

Phase	Degree of attention	Number of individuals involved	Degree of convergence on network issues	Network communication channels	Sphere of influence
Incubation phase	Very low	Few	Multipoint scatter	Single	Small
Outbreak phase	Increase rapidly	Increase gradually	Multi-aggregation	Increase gradually	Enlarge gradually
Diffusion phase	Increase stably	Continue to increase	Oligarchic gathering	Many	Enlarge rapidly
Decline phase	Decrease gradually	Decrease gradually	Scatter gradually	Reduce gradually	Diminish gradually

3.3   Diffusion Phase

During this period, the network becomes a "catalyst" of online trust crisis. The publicity of the crisis events is enlarged quickly in a short time, which is catalyzed and fermented through network environment, and attracts more individuals' concerns and participations. The number of individuals involved increase gradually, and the degree of attention increases sustainably, network medias change from niche to mass, the strong medias intervene actively, and negative information disseminating channels are formed rapidly, thus the enterprise sinks in the whirlpool of trust crises. Network public opinions are complicated, after the massive outbreak of online trust crisis, there will be "joint" effects in many fields, and increasingly more related things are involved widely. The enterprise's online trust crisis is most difficult to control in this phase.

3.4   Decline Phase

Finally the enterprise's online trust crisis enters the decline phase, mainly because of two reasons. One is that the individuals' views are shifted by new crisis events of

other organizations. The other is that the online trust crisis is treated effectively. The cyber hotspot sustains for a period of time, if new events emerge and new stimulus generated, a lot of individuals will automatically shift to new network issues, and they will pay decreasingly attentions to the old network hotspot, then it will be cooled, faded and fallen. When the enterprise's online trust crisis is treated effectively, the crisis will disappear gradually and the enterprise will enter into a new development stage. However, if the treatment was invalid, the residual factors of the online trust crisis will ferment and the online trust crisis will re-enter into a new life cycle.

4 The Framework of Enterprise's Online Trust Crisis Management Strategies

There are different characteristics in different stage of the enterprise's online trust crisis life cycle, and these characteristics determine the countermeasures used in the online trust crisis management. It is vital to find the countermeasures in accordance with the online trust crisis life cycle.

The fishbone diagrams are causal diagrams created by Ishikawa [33] in the 1960s. These show the causes of a specific event and each cause or reason for imperfection is a source of variation. A fish bone diagram is a common tool used for a cause and effect analysis, and it immediately sorts ideas into useful categories [34]. Nowadays, the fishbone diagram is widely used in the field of management.

According to the characteristics of each phase of online trust crisis and the basic principles of crisis management, drawing lessons from the idea of fishbone diagram, we construct the framework of enterprise's online trust crisis management strategies, as shown in Figure 2. The framework can provide references on the enterprise's online trust crisis management decision-making.
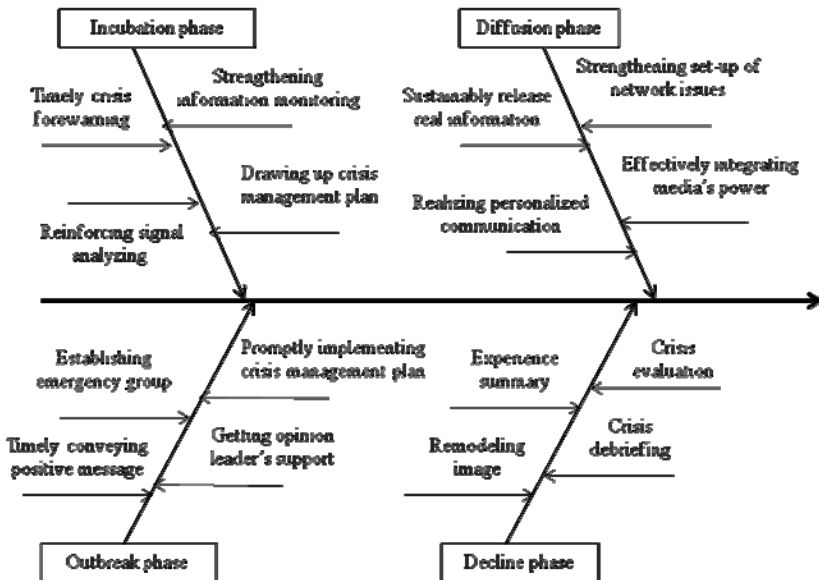

Fig. 2. The fishbone diagram of enterprise's online trust crisis management strategies

5 The Strategies of Enterprise's Online Trust Crisis Management

5.1 The Management in Incubation Phase

There are some signals to indicate the possibility of the online trust crisis though the great trust crisis events cannot yet happen during the incubation phase. At this time, the enterprise should pay more attention to the prevention of online trust crisis. If all kind of incentives which may induce the enterprise's online trust crisis could be monitored timely and the related signals could be analyzed carefully and forewarned effectively, then it could be possible to avoid the ordinary events suddenly upgrading to the burst of online trust crisis. The countermeasures in the incubation phase are discussed in more detail below.

5.1.1 Drawing up Crisis Management Plan

The enterprise needs to take the online trust crisis management into the overall work of enterprise's crisis management, and draw up the online trust crisis management plan based on the principles of integrity, predictability, initiative, operability and timeliness. It is crucial to make a plan for online trust crisis management, because it can effectively prevent the occurrence of some online trust crisis events, and avoid expanding the trust crisis as far as possible after the trust crisis is really happening. This is just a precaution for crisis management. Apart from definite management budget and segmentation of management target, there are two key points in online trust crisis management plan: one is the construction of online trust crisis management information system; the other is the construction of online trust crisis management team. The online trust crisis management information system is a subsystem of enterprise information system, which has the functions of trust crisis information collection, collation, analysis, identification, transmission, feedback, communication, publishing, recovery and assessment. The online trust crisis management team should establish the managing mechanism with centralized command and division of labor and cooperation. The online trust crisis management team should form strong professional personnel. There are some key functions of online trust crisis management team. Firstly, it should coordinate the relationships among internal departments, the enterprise and news media, and the enterprise and the social public. Secondly, it should collect, analyze, predict and evaluate various crisis-related information. Lastly, it should report the information to the enterprise decision-making setup.

5.1.2 Strengthening Information Monitoring

Although the occurrence of enterprise's online trust crisis may be sudden for unknown reasons with a certain degree of randomness, yet some information, views and attitudes will be displayed in network channels from the appearing of initial signals to the occurrence of online trust crisis. So the enterprise's online trust crisis can be monitored [35]. In order to get the signals of the enterprise's online trust crisis, the enterprise should monitor the external information related with the survival of the enterprise. The external information includes politics information, economy information, policy information, science and technology information, finance

information, market information, competitor information, supply and demand information, and consumer information. Additionally the enterprise should monitor the internal sensitive causes, which result from corporate mismanagement, business decision-making errors, the problems of product and service quality, financial crisis, the poor quality of staff, and the error of PR strategies.

5.1.3   Reinforcing Signal Analyzing

The analysis of cyber information monitored is a process to find problems and solve problems. After the collection of data, the analyzing process of information arrangement, identification, filtering and evaluation should be carried out. There are differences in the methods and focus of signals processing for different information communication platforms. As for network news data, the main core elements of the original should be maintained as far as possible, such as news title, source, release time, content, click number, reviewer, comment content and the comment number. As for BBS, blog, podcast, RSS, SNS, IM data and other social media, the original element and diffusion effects should be preserved as far as possible and formed the formatting information, such as the title of the post, the spokesman, the release time and content, content and number of replies, and so on. The abnormal information should be classified and analyzed timely, the hot spots, sensitive spots and dangerous spots, which may possibly cause online trust crisis, should be researched. The successful identification of potential and possible threats will lay the foundation for the enterprise's online trust crisis management.

5.1.4   Timely Crisis Forewarning

All signals analyzed and processed should be timely submitted to the crisis management team. The crisis management team should evaluate professionally the signals to determine whether the crisis forewarning is need. After an action decision, the online trust crisis forewarning should be realized automatically with the information technologies as one module of the enterprise information system. The forewarning indicators are built according to parameters such as the news source, news authority, comment number, release time and intensive degree, the viewpoint and orientation of the article or post, the degree of concern, and so on. This module owns the functions of semantic analysis, statistical analysis, comprehensive analysis and feature extraction by making full use of natural language processing, viewpoint mining, artificial intelligence, and visualization technology. In this way, the signals can be checked if they were in a normal range, once beyond a particular scope, the alarm is submitted to the online trust crisis management.

5.1.5   The Management in Outbreak Phase

This stage is especially critical for the enterprise's online trust crisis management. If the enterprise's online trust crisis could not be disposed improperly, the consequences of the trust crisis events will be in a deteriorating direction, the "heat" of online trust crisis will increase, and more individuals will participate in the discussion and communication. Thus, cyber will become the "blower" for the enterprise's online trust crisis, and the online trust crisis will be worsening. Following actions are needed.

5.1.6   Promptly Implementing the Crisis Management Plan

Once the online trust crisis is outbreaking, the enterprise should confirm rapidly and timely the crisis, find the source of crisis, determine the potentially affected the public, and implement promptly the online trust crisis management plan, assembling all kinds of resource to control the influence power of online trust crisis within a smaller range as far as possible. According to different crisis forms, the enterprise online trust management team should format the corresponding crisis control groups to provide effective organizational support. In addition, the enterprise online trust management team should strengthen the cooperation with government agencies, NGOs and media, and rely on the opinion leaders and the public to reduce the damage to a minimum.

5.1.7   Getting the Support of Opinion Leader

Opinion leader is an active media user who interprets the meaning of media messages or content for lower-end media users [36]. There is a lot of promoting by opinion leaders almost behind every network hot issue. In some events, the viewpoints of opinion leaders can play and unexpected role on the settlement, because as the person concerned in the event, the point of view of the enterprise is difficult to get fully recognized by individuals. Therefore, the enterprise should actively win the support of opinion leaders and make full use of the third-party persuading role of opinion leaders, encouraging opinion leaders to guide online speech through blogs, podcasts, SNS, RSS, and other social media. The opinion leaders should be the strong support for the enterprise and the external opinion. At the same time, the enterprise should cultivate actively its own "opinion leaders" to form a positive guiding force in the "new opinion stratum".

5.1.8   Timely Conveying Positive Message

Winning the time is equal to winning the image. There may not be enough reliable information at the onset of the crisis. In order to avoid information vacuum and rumors flying long, the enterprise must strive for controlling the situation in a short time and endeavor to communicate with public in the first time, conveying positive messages, indicating attitudes, informing of the activities being adopted. Then the public will feel the enterprise's responsibility consciousness and public philosophy, and they will be in favor of the enterprise psychologically. The key point to keep the initiative in information release is that the enterprise itself should be the first hand information release source and provide the necessary background information to media and public as much as possible, not giving too much playing space to media. The enterprise should inform news media about the crisis basic facts and the management countermeasures in the shortest period of time, and clarify the stance and attitude to get the trust and support of the media and lead actively public opinions. In such a way, the enterprise will quickly control the situation by not giving up any rights of speech.

5.1.9   The Management in Diffusion Phase

Due to the openness, timeliness and interactivity of Web 2.0, there are cascading effects during the diffusion phase of online trust crisis. It is difficult to manage online

trust crisis in the diffusion phase. In addition to adhering continuously the countermeasures mentioned above, the enterprise should also do the following works.

5.1.10   Effectively Integrating Media's Power

The enterprise online trust crisis management team should actively coordinate the relationship with the mainstream traditional media and online media. The enterprise can communicate and dialogue with individuals frankly in proper communicating atmosphere with unblocked information channels. During the communication, the positive interaction between the enterprise and the society will be formed, and the chaos of social public caused with blocking messages and uniformed information will be avoided. It is very important to ensure the rights of speech of individuals, which can overcome the desire for fear or revenge of public to reduce the instability factors. In this way, the public's resentment on the crisis event can be led to the rational thinking of the nature and solutions of the event. And then the attitudes and behaviors of individuals will be advantageous to resolve online trust crisis and reduce the negative influence and loss.

5.1.11   Sustainably Release Real Information

The enterprise should release information sincerely, meet and maintain the public's right to know, winning opportunities for subsequent disposal of the trust crisis. The online trust crisis can be led and mediated in the direction of control by disclosing relevant information, and the social anxieties will be reduced. The enterprise can sustainably release real information and enhance the transparency of information through the enterprise's website, enterprise's news spokesman, hotlines, being a guest on network media and social media.

5.1.12   Strengthening Set-up of Network Issues

The primacy effect [37], in psychology and sociology, is a cognitive bias that results in a subject recalling primary information presented better than information presented later on. In the network era, the energy of primacy effect increases in hundreds or thousands times in the process of network communication. It is an effective way to guide the cyber opinions by setting up the official network issue. When the online trust crisis is breaks out, the enterprise should try its best to set the related subjects or topics in the first time consciously. On one hand, the attentions of individuals will be directed to the special themes. On the other hand, the diffusion of online trust crisis will be decreased as much as possible. The enterprise can actively get the rights of speech and guide the development of network opinions by setting communicating topics initiatively, making the network discussion become more efficient, hierarchical, systematic and controllable.

5.1.13   Realizing Personalized Communication with Individuals

In order to achieve the communicating goals in the situation of crisis, the target audience should be divided into several types and each type should adopt different communicating method and channel. The classification standards include the value, behavior habit, life style, education degree, racial, economic status, age, gender, and information selection habit of individual. Aiming at the personalized communication

needs of each type of target audience, the enterprise should choose the proper transmission time, transmission channel, information content and expression forms based on satisfying the targeted communication. Of course, these all depend on information technologies.

5.2   Management in Decline Phase

Whatever the cause, when the enterprise's online trust enters into decline phase, the enterprise should carry out crisis evaluation, crisis debriefing and image remodeling.

5.2.1   Crisis Evaluation

The crisis evaluation includes the evaluation of basic support, the evaluation of disposal process and the evaluation of settlement results. The evaluation of basic support looks for loopholes of online trust crisis monitoring, forewarning and management plan to make up the shortfalls. The evaluation of disposal process can help the enterprise to improve the online trust crisis management process and enhance the enterprise's ability to cope with the online trust crisis in the future. After the online crisis trust, the enterprise should track and mend continuously the settlement results, and think over the recovery measures. The evaluation of settlement results should be fed back to the online trust crisis management plan, perfecting the plan, and providing effective basis for the future online trust crisis.

5.2.2   Crisis Debriefing

The crisis debriefing is an inevitably phase in online trust crisis management. The work of crisis debriefing is an important mechanism the enterprise tries its best to recover the cyber order to its normal state and prevent the germination of new online trust crisis. On one hand, if the enterprise really produced the trust events and had negative effects on social public, the enterprise should take responsibility and apologize actively and initiatively to get their understanding. On the other hand, if some organizations and persons violate laws, regulations or the network obligation and cause damages to the enterprise, the enterprise should actively investigate and pursue such organizations' or persons' legal liabilities.

5.2.3   Remodeling Image

The destructiveness given by online trust crisis is mainly manifested in the deterioration of the enterprise's image. Thus, when the online trust crisis enters into the decline phase, the enterprise must try its best to reshape the corporate identity. The process of remodeling image is actually the process that the enterprise pursues self-improvement and constantly gets the public's recognition, understanding and support. On one hand, the enterprise should complete the internal works to truly provide high-quality products and service to society. On the other hand, the enterprise must maintain good relations with all kinds of social public, planning and implementing a serial of PR activities manifesting the brand reputation and corporate identity, product promotion, and public benefit activities reflected the enterprise's social responsibility.

6   Conclusions

With the rapid development of Internet and telecommunication network, the occurrences of online trust crises become increasingly more frequent. The negative influences and destructive effects caused by online trust crises are growing. We study the phases of enterprise's online trust crisis life cycle and put forward the frame of enterprise's online trust crisis management strategies based on the characteristics of online trust crisis in incubation phase, outbreak phase, diffusion phase and decline phase, which may provide some theoretical supports for enterprise's online trust crisis management. Crisis management is also called crisis communication management [4]. The emphasis of enterprise's online trust crisis management is to achieve and enhance communication with the public. Communication becomes the core of management in each stage of online trust crisis cycle. Of course, the enterprise's online trust crisis management requires a lot of manpower, material and financial resources, and thus it could be difficult to realize for micro and small enterprises (MSEs). Based on recent cases, Internet users pay more attention to the production and operation of well-known enterprises, and well-known enterprises have become the main body of the outbreak of online trust crisis. All well-known enterprises should attach importance to online trust crisis management.

References

1. Internet Users in the World Distribution By World Regions-2012 Q2 (December 26, 2012), `http://www.internetworldstats.com/stats.htm`
2. 33th statistical report on the Internet Development in China, `http://www.cnnic.net.cn`
3. Global e-commerce sales will top $1.25 trillion by 2013, `http://www.internetretailer.com/2012/06/14/global-e-commerce-sales-will-top-125-trillion-2013`
4. The transactions of e-commerce market in China amounted to 5.6 trillion Yuan in the first three seasons, `http://finance.sina.com.cn/chanjing/cyxw/20121127/153913813624.shtml`
5. Liu, C., Marchewka, J.T., Lu, J., Yu, C.: Beyond concern: a privacy–trust–behavioral intention model of electronic commerce. Information Management 42, 127–142 (2004)
6. Pavlou, P.A., Liang, H., Xue, Y.: Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. MIS Quarterly 31, 105–136 (2007)
7. Luo, X., Lib, H., Zhang, J., Shimd, J.P.: Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. Decision Support Systems 49, 222–234 (2010)
8. Mesch, G.S.: Is online trust and trust in social teams associated with online disclosure of identifiable information online? Computers in Human Behavior 28, 1471–1477 (2012)
9. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Academy of Management Review 20, 709–734 (1995)
10. Bachmann, R.: Trust, Power and Control in Transorganizational Relations. Organization Studies 22, 337–365 (2001)

11. Devosk, T., Spini, D., Schwartz, S.: Conflicts among human values and trust in institutions. British Journal of Social Psychology 41, 481–494 (2002)
12. Alesina, A., Ferrara, E.: Who trusts others? Journal of Public Economics 85, 207–234 (2002)
13. Rousseau, D.M., Stkin, S.B., Camerer, C.: Not so different after all: a cross-discipline view of trust. Academy of Management Review 3, 393–404 (1998)
14. Beldad, A., Jong, M., Steehouder, M.: How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior 26, 857–869 (2010)
15. Midha, V.: Impact of consumer empowerment on online trust: An examination across genders. Decision Support Systems 54, 198–205 (2012)
16. Seeger, M.W., Sellnow, T.L., Ulmer, R.R.: Communication, organization and crisis. Praeger, Santa Barbara (2003)
17. Luo, X.M.: Trust production and privacy concerns on the Internet A framework based on relationship marketing and social. Industrial Marketing Management 31, 111–118 (2002)
18. Wang, Y.D., Emurian, H.: An overview of online trust: concepts, elements, and implications. Computers in Human Behavior 21, 105–125 (2005)
19. Gefen, D., Benbasat, I., Pavlou, P.: A research agenda for trust in online environments. Journal of Management Information Systems 24, 275–286 (2008)
20. Beldad, A., Jong, M., Steehouder, M.: How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior 26, 857–869 (2010)
21. Benedicktus, R.L.: The effects of 3rd party consensus information on service expectations and online trust. Journal of Business Research 64, 846–853 (2011)
22. Bock, G.W., et al.: The progression of online trust in the multi-channel retailer context and the role of product uncertainty. Decision Support Systems 53, 97–107 (2012)
23. Kim, Y.A., Ahmad, M.A.: Trust, distrust and lack of confidence of users in online social media-sharing communities. Knowledge-Based Systems 37, 438–450 (2013)
24. Heath, R.: Dealing with the complete crisis-the crisis management shell structure. Safety Science 30, 139–150 (1998)
25. Mak, H.Y., et al.: Building online crisis management support using workflow systems. Decision Support Systems 25, 209–224 (1999)
26. Murray, W.B., Foster, P.A.: Crisis Resource Management Among Strangers: Principles of Organizing a Multidisciplinary Group for Crisis Resource Management. Journal of Clinical Anesthesia 12, 633–638 (2000)
27. Ryzenko, J., Smolarkiewicz, M.: Space-enabled information environment for crisis management. Scenario-based analysis and evaluation in an operational environment. Acta Astronautica 66, 33–39 (2010)
28. Christine, M., Pearson, S.: Amy Sommer. Infusing creativity into crisis management: An essential approach today. Organizational Dynamics 40, 27–33 (2011)
29. Speakman, M., Sharpley, R.: A chaos theory perspective on destination crisis management: Evidence from Mexico. Journal of Destination Marketing & Management 1, 67–77 (2012)
30. Sardouk, A., et al.: Crisis management using MAS-based wireless sensor networks. Computer Network (2012),
    http://dx.doi.org/10.1016/j.comnet.2012.08.010
31. Chou, D.C., Chou, A.Y.: Information systems outsourcing life cycle and risks analysis. Computer Standards & Interfaces 31, 1036–1043 (2009)

32. Tan, C.H., Zeng, Y.T.: Research on the Discrimination of Enterprise Online Trust Crisis Based on "Twice Evaluation" Mechanism. Information Science 29, 1815–1819 (2011)
33. Kaoru, I.: Guide to Quality Control, Asian Productivity Organization. UNIPUB. (1976)
34. Nancy, R.: Tague's The Quality Toolbox, Second Edition. ASQ Quality Press, Milwaukee (2004)
35. Tan, C.H., Wang, X.: Research on the Model of Enterprise's Online Trust Crisis Prevention Based on Ontology and Web Mining. Information Science 29, 1559–1564 (2011)
36. Gnambs, T., Batinic, B.: Convergent and discriminant validity of opinion leader: Multitrait-multimethod analysis across measurement occasion and informant type. Journal of Individual Differences 39, 94–102 (2011)
37. Jones, E.E., et al.: Pattern of performance and ability attribution: An unexpected primacy effect. Journal of Personality and Social Psychology 10, 317–340 (1968)
38. Herrero, A.G., Pratt, C.B.: An Integrated Symmetrical Model for Crisis-Communications Management. Journal of Public Relations Research 8, 79–105 (1996)