Cyber Crisis Management: A decision-support framework for disclosing security incident information

Olga Kulikova, Ronald Heil
ICT Security & Control
KPMG
Amstelveen, the Netherlands
Email: {Kulikova.Olga,Heil.Ronald}@kpmg.nl

Jan van den Berg, Wolter Pieters
Faculty of Technology, Policy, and Management
TU Delft
Delft, the Netherlands
Email: {J.vandenBerg,W.Pieters}@tudelft.nl

***Abstract*—The growing sophistication and frequency of cyber attacks force modern companies to be prepared beforehand for potential cyber security incidents and data leaks. A proper incident disclosure strategy can significantly improve timeliness and effectiveness of incident response activities, reduce legal fines, and restore confidence and trust of a company's key stakeholders. In this paper, four factors that shape organizational preferences regarding incident information disclosure are introduced. Together, they create a set of challenges for a company when deciding to whom, when, what, and how to share cyber security incident information. We further propose a decision-support framework that provides step-by-step guidance for organizations to address these challenges, and develop an appropriate incident disclosure strategy.**

***Index Terms*—Cyber security, incident response, information disclosure, internal and external stakeholders.**

I. Introduction

Every incident creates a need for information, both for people dealing with it inside the company as well as outside audiences [1]. Incident information disclosure, thus, is an essential part of crisis communications, which can "reduce and contain harm, provide specific information to stakeholders, initiate and enhance recovery, manage image and perceptions of blame and responsibility, repair legitimacy, generate support and assistance, explain and justify actions, apologize, promote healing, learning, and change" [2]. At the same time, incident information disclosure is a complex task since it depends on both organizational internal factors and external ones, such as "culture, legal system, and institutional background" [3].

Speaking about cyber incidents, in 2011, 92% of cyber security breaches were discovered by a third party [4], meaning that in the majority of cases a company will not be able to hide what happened and will have to establish a dialogue with external parties. 85% of all incidents took weeks or more to discover thus affecting more stakeholders and causing more harm, so a company has to be prepared to give a proper incident explanation in order to avoid public censure. Existing and upcoming regulations make the situation even more difficult requiring the notification of regulatory authorities, law enforcement, or the public in such cases like personal data breaches [5].

Not having processes in place to ensure timely and consistent communication with stakeholders can lead to damaging consequences. Bad communications can contribute to overall confusion about the situation among key audiences, initiate rumors, and trigger a sell-off of company's shares [6]. In contrast, clear communications can help to quickly engage internal and external stakeholders in incident response, and help them make sound decisions faster. It will increase overall transparency of an organization, which is beneficial for any company in times of new disclosure regulations and increased public scrutiny [7]. A security incident disclosure plan would guarantee the described benefits and limit the chance of further incident escalation.

The main goal of this paper to introduce a decision-support framework that provides clear guidance for organizations in developing an adequate incident disclosure strategy. To do so, a set of factors is identified (in section II) that influence the organizational preferences regarding incident information disclosure. In section III, we combine these with four different strategy questions, in order to create an overview of all disclosure challenges. In section IV, the time dimension is added, which finally results into the aimed incident disclosure framework in section V. Conclusions are drawn in section VI.

II. Factors Influencing Incident Disclosure

Companies disclose cyber security incident information to certain stakeholder groups for a variety of reasons, such as complying with legal requirements by notifying controllers, asking for help of supporters, or restoring reputation in the eyes of the value chain and media [5, 8, 9]. Regardless the motive, these activities will require different approaches in terms of notification audience, time, content, and methods, which complicates the decision-making process of developing a unified incident disclosure strategy. A question arises: what are the main factors that shape organizational preferences regarding when, what, how, and with whom to share security incident information?

978-0-7695-5014-5/12 $26.00 © 2012 IEEE
DOI 10.1109/CyberSecurity.2012.20

According to [10], disclosure strategies are shaped "by existing regulations and by the costs associated with disclosure, such as information collection and processing costs, litigation costs, and proprietary (i.e., competitive disadvantage and political) costs." Public pressures from media and reputational concerns are mentioned by [11] and [12] as another determinant of organizational disclosure strategy. In general, these claims correlate with the findings of [13], who, in their research on data breach notifications, conclude that organizational disclosure strategies are influenced by three main factors, namely, *regulatory, economic,* and *reputational factors*.

Still, the process of incident response itself can serve as a motivation to disclose security incident information. More and more papers on security incidents emphasize that information sharing is a key component to successfully mitigate harm caused by security incidents, and also to reduce the chance of their occurrence in the future [14, 15]. In times when companies lack employees that can deal with the whole scope of possible security incidents, information sharing among companies and government agencies on security incidents can become a 'life saver' in case of advanced cyber attacks [8, 15]. As a consequence, besides three factors previously identified by [13], *harm mitigation and prevention* can also serve as a determinant of a company's cyber security incident disclosure strategy. Altogether, we conclude that disclosure strategy can be influenced by four factors: *harm mitigation and prevention, regulatory compliance, cost-efficiency,* and *reputation*. The name 'cost-efficiency' is chosen rather than 'economic' to get a better representation of what is meant by this factor - ensuring that the perceived benefits of the disclosure exceed the perceived costs.

The rest of the section explains why each dimension is a key element in making decisions about cyber incident notifications to internal and external stakeholders.

A. Harm mitigation and prevention

Incident disclosure helps to *mitigate* harm by increasing situational awareness within a company. Better situational awareness allows employees to evaluate potential risks, and then prepare and execute courses of action without negative consequences to the enterprise [16]. For example, an internal team dealing with a cyber incident should be constantly aware of its business seriousness. Without proper understanding of the incident's impact on the organization, employees can make decisions that will further aggravate a company's already precarious position. Sensitive information can be released to outside parties through internal negligence, which will lead to further escalation of the incident and greater disruptions.

Incident disclosure can help to *prevent* future harm by making employees learn from the bad experience, or by voluntarily sharing incident information across industries, in order to improve overall cyber security [13, 15]. Hausken, in his paper on information sharing among firms and cyber attacks [17], showed that organizational aggregate defense can be improved through exchange of information with other companies, when security investments become too costly.

B. Regulatory compliance

Regulatory compliance can prevail in the organizational decision-making process around an occurring security incident, also with respect to incident information disclosure [18]. Laws increasingly require and advise organizations to be more proactive and open to the public in the face of cyber attack threats, and disclose cyber security incident information [19]. The draft EU data law, for example, will require notification of any personal data breach to certain authorities within very tight timeframes of 24 hours. If it is not the case, notification delays should be given a proper explanation [20].

Currently, the requirements on disclosure of cyber security incident information exist when either 1) there is leak of personal data or 2) cyber incident presents a material threat for an organization. With respect to personal data breaches, some regulations concern only specific industries, like financial and health institutions, or telecom providers [5]. These regulations require that notifications are provided either to the individuals affected, state regulatory agencies and law enforcement, or only to individuals affected. The failure to notify these entities may result in big fines to a company. Hence, it is of high importance to make an organizational disclosure strategy consistent with current laws, and review it on an ongoing basis since regulations change.

Regarding cyber incidents as a material threat, the U.S. Securities and Exchange Commission (SEC) requires the disclosure of material events for every listed company on the New York Stock Exchange (NYSE) [21]. Before last year, companies used to exclude cyber incidents from the scope of the SEC requirement since it did not explicitly state otherwise. To clarify the situation, the SEC issued guidance on October 13, 2011, which emphasizes that cyber-risks should be disclosed as any other type of incident [22]. Since then, a company has to determine the correct definition of what constitutes a material cyber security incident and disclose them in annual reports and certain forms [23].

What complicates the regulatory compliance in terms of incident disclosure, is that cyber transactions are not tied to a particular location as laws usually are [8]. They occur globally; hence organizations operating within multiple jurisdictions must comply with a "lengthy list of regulations varied depending on a type of business, vertical industry, and the geographic location." [5] Team members from one country may initiate actions that are illegal in other jurisdictions, so communication mechanisms should be established that create a constant awareness of an incident's geographic specifics. A company must be familiar with requirements of all countries it operates in and understand how cyber incidents fall under the scope of these regulations. If a cyber attack results in a leak of personal data, an organization will have to comply with notification requirements of all countries whose citizens are involved in the incident.

C. Cost-efficiency

Financial resources are another determinant of an organization's choice of their disclosure strategy. According to [13], "a firm seeks to calibrate security expenditures according to the level of legal liability and the financial risks that they bear from leaked information." A company may not be able to adopt a particular disclosure strategy, e.g. due to further costly lawsuits; in this case the less-expensive strategy will be chosen. In short, incident information disclosure should bring more benefits to a company than associated costs. In this sense, financial constraints often create so-called disclosure disincentive: a company will prefer to stay silent if there is no external discovery of an incident [13]. This avoids costly legal actions, and allows dedicating organizational resources and time to actual incident response, instead of dealing with media, law enforcement, and other agencies. It will also reduce the chance of customers or investors switching to a competitor in order to feel more secure.

With respect to cyber security attacks it might be expected that quick notification of affected parties is in the company's best interest. However, according to the Ponemon Institute's annual investigation [19], quick incident response activities can cause cost inefficiencies resulting in a firm overpaying for data breach mitigation procedures. At the same time, too late notifications can result in the irreparable damage of company's reputation, loss of clients and public confidence. Thus, a *timely* and not *speedy* incident response is needed [24], and how to determine these "timely" frames is becoming a big issue, to assure both cost-efficiency and safety of the company's reputation.

D. Reputation

The last key focus of a company when choosing its disclosure strategy is that it should contain the damage to reputation, and restore the confidence and trust of key stakeholders.

Reputation is a valuable asset for any organization: it can attract new customers and talented employees, generate new investments and create competitive advantages [12]. A good reputation provides enhanced legitimacy, lower operations costs, greater market acceptance of new products, and an enhanced ability to withstand times of trouble. At the same time, a damaged reputation can cause consequential loss of customers and investors and higher public scrutiny of further business operations [25]. As a result, companies quite often are more afraid of a damaged reputation caused by bad publicity than the actual financial losses while dealing with the incident [19]. According to a recent survey from *PwC*, reputational damage is the biggest fear of 40% of respondents when experiencing cyber security incidents [26].

The reason of such fear is that nowadays reputation is very exposed to criticism. The growing number of media sources like blogs and social networks allows negative information and rumors to be spread in a matter of seconds [12, 27]. Plus, there is an increasing number of hacktivists attacking companies specifically to share negative information about them using media. Media, at the same time, has become the main source from which external stakeholders get the information about organizations [25]. Consequently, they will tend to adopt the media's view on an incident, and a company in turn will find it difficult to change already formed perceptions of an external audience during a crisis.

Hence, incident information disclosure must reflect extant perceptions about the company. If regulations allow, a company may prefer to keep tight control on its incident information disclosure and choose a non-disclosure strategy which avoids bad publicity [13]. At the same time, if a cyber incident is discovered externally, no matter how much a company wants to keep quiet, as [28] fairly notices: “Silence... can prove to be a brand's most damaging strategy.”

III. Cyber Incident Disclosure Challenges

The four introduced factors create the conditions that should be taken into account when a cyber security incident with possibly high impact occurs and the organization at stake needs to define an adequate response. Among others, it needs to assess the situation as soon as possible and make a set of adequate decisions in order to mitigate the possible impact of the occurring incident. The latter includes the implementation of an appropriate information disclosure approach.

With respect to the information disclosure, the organization at stake starts facing decision problems regarding the audience and timing of notifications, the notification content and methods of information disclosure. The relevant questions can be grouped into the following categories:

- *“Whom”* category applies to audience receiving incident information notifications. It can be various entities such as the company’s customers, suppliers and partners; entities that help a company to respond to a cyber attack; government agencies, media, and the general public.
- *“When”* category refers to the timings when security incident information is disclosed. It includes notification triggers, speed with which information is disclosed, and frequency of the information updates.
- *“What”* category describes content of what is being disclosed - the amount of information to release as well as the exact message.
- *“How”* category refers to the methods by which security incident information is disclosed. A company may use different communication channels for this purpose, like e-mail, phone, website postings, newspapers, television, etc.

Below, in Table I, we summarized challenges created by these four categories, in combination with the factors of the previous section. Together, these challenge categories create a decision-making landscape of organizational security incident information disclosure. Every challenge should be addressed and solutions should be evaluated in order to choose the most appropriate disclosure strategy, and therefore ensure an effective cyber incident management process.

Currently, there is no commonly agreed strategy on how to address the identified challenges. Every incident has a unique set of traits [8], plus different organizations follow different business models [29], so the academic and practitioner experts agree that disclosure strategies vary widely across organizations. Moreover, they would be adjusted on case-by-case approach for every particular incident [8, 9, 13].

TABLE I. INCIDENT INFORMATION DISCLOSURE CHALLENGES.

	"To whom"	**"When"**	**"What"**	**"How"**
Harm mitigation and prevention	Identifying the right stakeholders to be informed for effective incident response and harm mitigation	Identifying when to release notifications to facilitate the incident response process	Creating a proper notice to each stakeholder group, so they can evaluate risks and take the right course of actions	Identifying notification methods that assure speed and correctness of the disclosed information
Regulatory compliance	Identifying who must be notified due to legal requirements, if any	Identifying the specific timings of stakeholders notification required by law, if any	Identifying what information must be in the notice due to legal requirements, if any	Identifying what notification methods to use due to legal requirements, if any
Cost-efficiency	Assuring that the scope of notified audiences reflects the severity of the incident	Assuring that the disclosure times do not further aggravate a company's situation	Assuring that information disclosed does not create further financial losses	Identifying cost-efficient notification methods
Reputation	Identifying stakeholders who can help restore reputation, and those who can damage it	Identifying the appropriate timings of incident notifications that is beneficial for a company's reputation	Identifying what disclosure content can help restore reputation, and does not damage it	Identifying notification methods that are beneficial for a company's reputation

Still, as was discussed in the previous section, having a generic disclosure plan is a crucial step in a company's efforts to successfully manage a cyber security incident. A company must have some decision-making support mechanism, or framework, that will help to adjust this plan for every cyber incident situation.

IV. THE GENERIC INCIDENT NOTIFICATION TIMELINE

The creation of a generic timeline of an incident disclosure process was a starting point in the design of a decision-support framework. The timeline allowed mapping out, to the extent possible, the common steps of the incident disclosure process and using them as a basis for the framework.

The timeline, shown in Fig. 1, shows the main incident disclosure activities, internal and external, with respect to an evolving incident lifecycle[1]. Every incident is unique and managed differently, but there are certain steps that stay relatively constant with every cyber security incident:

Step 1. The incident impact assessment and the formation of an incident response team (IRT) in order to initiate the response process and harm mitigation;

Step 2. The IRT's further assessment of the incident specific details as well as organizational priorities regarding the incident response;

Step 3. The incident disclosure strategy development and realization based on the previous assessment;

Step 4. Post-disclosure learning.

Together, these steps form the foundation for the framework design described in the next section.

V. THE DECISION-SUPPORT FRAMEWORK

When a real incident happens, the company will modify the timeline to reflect the unique nature of the incident by following the procedures proposed by the decision-support framework. In this article, a flowchart diagram, shown in Fig. 2, is used to illustrate the framework approach. It follows the four common steps introduced in the previous section.

The subsections below describe every step in the flowchart, by giving an explanation on how every process works, together with the particular examples and overall justification of their presence in the flowchart. For easier reference, every process is assigned a letter, starting with (A) and ending with a (J).

First step. Incident Response Team formation.

As security incidents vary widely in their severity, the composition of the incident response team should reflect the impact the incident has on the organization. Small virus outbreaks can be managed by one or two employees without necessity in further notifications, while incidents involving external people require assistance of HR, Legal or the Communication coordinator. This fact is recognized by many organizations worldwide that employ business impact assessment in their processes. After a security incident is confirmed by a help-desk or other IT Service (A), it is necessary to assess its adverse effect on the company, and assign the appropriate impact level (B). Once the level is determined, the incident response group needs to be formed in accordance with the level, in order to initiate the incident management process (C).

A: Security incident confirmed

In the first stage, an incident is confirmed either through internal review or through notification by external parties.

[1] The six stages of crisis: *warning, risk assessment, initial response, management, resolution, recovery and learning,* are adapted from the paper "Six Stages of a Crisis Model" introduced by Everbridge [32].

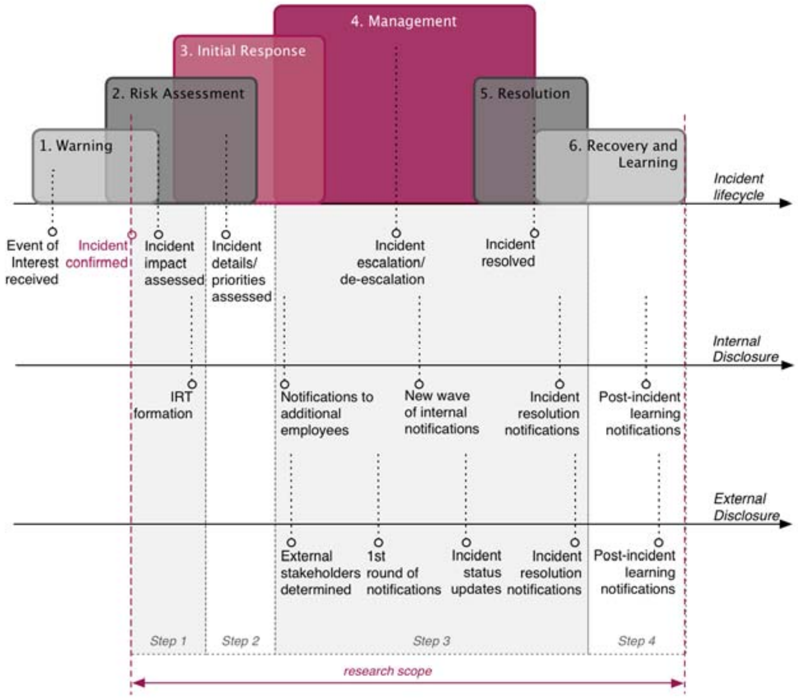
4. Management
3. Initial Response
2. Risk Assessment
5. Resolution
1. Warning
6. Recovery and Learning
Incident lifecycle
Event of Interest received
Incident confirmed
Incident impact assessed
Incident details/ priorities assessed
Incident escalation/ de-escalation
Incident resolved
Internal Disclosure
IRT formation
Notifications to additional employees
New wave of internal notifications
Incident resolution notifications
Post-incident learning notifications
External Disclosure
External stakeholders determined
1st round of notifications
Incident status updates
Incident resolution notifications
Post-incident learning notifications
Step 1
Step 2
Step 3
Step 4
research scope

Fig. 1. The generic incident notification timeline.

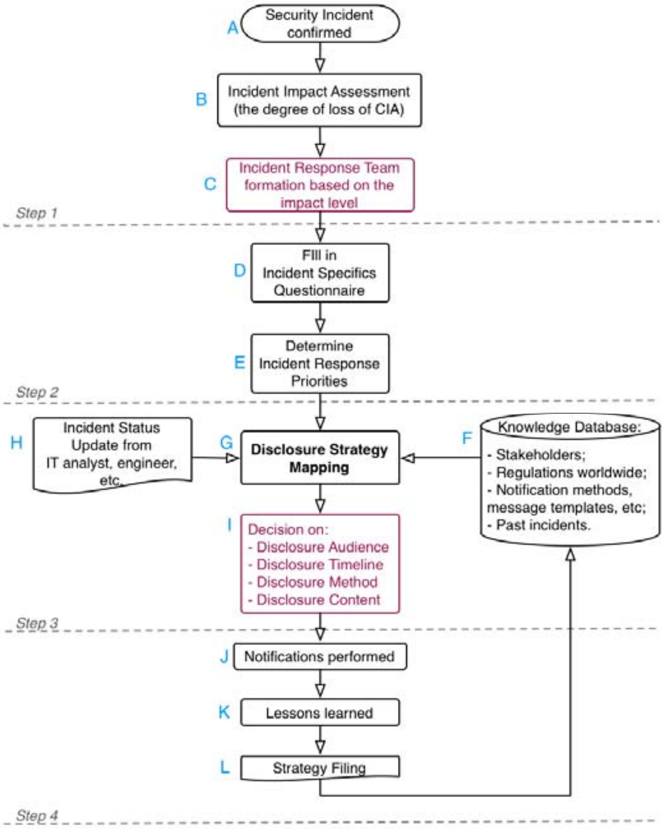
A
Security Incident confirmed
B
Incident Impact Assessment (the degree of loss of CIA)
C
Incident Response Team formation based on the impact level
Step 1
D
FIll in Incident Specifics Questionnaire
E
Determine Incident Response Priorities
Step 2
H
Incident Status Update from IT analyst, engineer, etc.
G
Disclosure Strategy Mapping
F
Knowledge Database:
- Stakeholders;
- Regulations worldwide;
- Notification methods, message templates, etc;
- Past incidents.
I
Decision on:
- Disclosure Audience
- Disclosure Timeline
- Disclosure Method
- Disclosure Content
Step 3
J
Notifications performed
K
Lessons learned
L
Strategy Filing
Step 4

Fig. 2. Incident disclosure strategy flowchart.

B: Incident impact assessment of the loss of confidentiality, integrity, and availability

Different organizations may have different approaches in assessing the impact of the incident. In general, the impact of the incident is captured using Confidentiality, Integrity, and Availability (CIA) impact scorings that reflect the impact of loss of confidentiality, integrity, and availability of a company's information systems [30]. For the fast and correct IRT formation, a company may develop an impact assessment that considers confidentiality, integrity, and availability of highly important servers or systems, which, in case of the incident, will immediately escalate the impact level to the maximum one. The list of all servers with their importance level can be developed in advance, for later reference.

C: The IRT formation.

Organizations should have a pre-defined list of employees that are involved in the incident response depending on its impact level. In the case of advanced cyber security incidents, the team should be cross-functional and involve (at least) coordinators from the incident response management team, the privacy office, corporate communications, senior management, and the legal department.

Second step. Assessment of the incident specifics and organizational priorities

D: Incident Specifics Questionnaire.

Once the initial incident response team has been defined, the next question would be whether specific internal specialists are still required to join (e.g. in case of a wide media incident coverage, it would be essential to invite the Public Relations coordinator), and whether external disclosure is required. The answers completely depend on the incident, hence a process in place is required that will help to summarize all key incident details that affect the disclosure decision.

In this paper, a list of initial questions to assist in describing the incident specifics is proposed, called *Incident Specifics Questionnaire*. Answers on these questions will very likely influence the disclosure decision of a majority of companies. The list can be extended or modified with more precise questions depending on the organizational industry and the types of data it operates with.

- How was the incident discovered? (e.g., internally, by law enforcement, media, or hacker)
- Which locations does the incident cover?
- What is the attack result? (e.g., unauthorized access, misuse of data, disruption of services)
- Does the incident present a material risk?
- Is external help required for the incident mitigation?
- Can voluntary sharing anyhow benefit the company?

By filling in this questionnaire, a company will have a set of data that can already determine a certain incident disclosure strategy after comparing the data with the existing knowledge base on incident information disclosure, described in the next step.

E: Incident Response Priorities.

Every security incident creates certain demands for a company regarding incident information disclosure. These demands are clarified by collecting information about the incident with the help of the incident specifics questionnaire. At the same time, organizations themselves have certain preferences on how to disclose the incident information. As was discussed earlier there are four factors that form these preferences: harm mitigation, regulatory compliance, cost-efficiency, and reputation. The disclosure strategy should not be based solely on what is required; it should deliver value for an organization and help to mitigate harm caused by the security incident. Thus, besides the incident details, it is also essential to know what preferences an organization has with respect to the particular incident.

Gartner, in their research on security incident preparation, states that before a security officer can define an appropriate response to an incident, there should be a complete understanding of the enterprise's priorities [31]. They suggest using a tool called *incident response priority sliders,* shown in Fig. 3, that forces choices about the organizational preferences. The idea is that it is not possible to put all sliders on maximum; an organization does not have enough resources to focus on all objectives listed on the left side. Steps towards maximum for one objective will require steps backwards for the other ones.

Incident response priority sliders can be applied to determine a company's priorities regarding the particular incident disclosure. They can help to clearly mark out what an organization wants to achieve with its disclosure strategy. For example, a company that put sliders in a way as it shown in Fig. 3, is mainly interested in the restoration of all affected operations and the identification of the incident cause. Giving notice to regulatory authorities or affected individuals is postponed, as reputation or financial concerns are not among its priorities. After clarifying these preferences, a company may adopt a disclosure strategy that will claim e.g. the two-week delay in notifying affected customers to ensure that the final statement about the cause of the incident is correct.

Incident response priority sliders together with the incident details compose a complete set of prerequisites that will influence the choice of the organizational incident disclosure strategy. In order to properly arrange sliders, an IRT will need the information about the incident specifics. That is why in the flowchart, the process of adjusting priorities follows the questionnaire.

Third step. Incident Disclosure Strategy Mapping

After the incident details and a company's priorities have been identified, the IRT can start the actual process of arriving at the incident disclosure strategy. In order to find an optimal solution, an analyst should define how the data gathered before (D, E) influences the way the disclosure should be performed. It is possible by mapping the collected incident data with the information from the Knowledge Database (F),

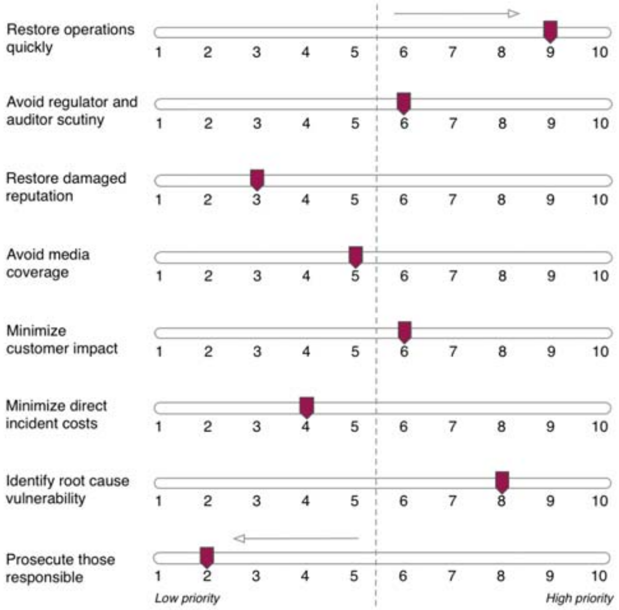

Fig. 3. Incident response priority sliders. Based on [31].

which stores the up-to-date lists of regulations, stakeholders' contacts, notification scenarios and message templates, etc. This process is called Disclosure Strategy Mapping (H); the outcome of the process (I) is an optimal incident disclosure strategy.

F: Knowledge Database.

The content of the knowledge database can be different depending on the company. There are, however, several databases that must be implemented to guarantee the compliance and proper stakeholders sampling. A company should maintain and regularly update the database of applicable regulations across all operational locations, which will allow one to quickly determine whether external notifications are required, to whom, how soon, and with which content. Such a database will allow a company to eliminate the need to constantly contact external parties asking for their legal advice. Then, without a comprehensive knowledge on stakeholders that can in any way assist in incident response, or be a subject to potential incidents, a company will not be able to determine the appropriate disclosure audience when a crisis strikes, and thus the chances to effectively mitigate the harm after incidents will be significantly reduced.

A company will eliminate some time demanding work during an actual incident if it prepares beforehand an incident disclosure database with such information as incident notification templates, available communication channels depending on the location, past incidents and the way they were disclosed, etc. Message templates, for example, can be prepared for the location specific notifications, or the notifications to the most important relationships. In general, the incident disclosure database can store any tactical information a company finds appropriate for the possible incident scenarios, for further reference in case of a real incident. It is a good solution to consider specifics of cyber incidents too, by adding the information particularly tailored to cyber incident scenarios, like a number of third-party contacts that are specialized in cyber forensics, or message templates to customers on what to do in case their bank credentials have been compromised.

It is not in the scope of this research to discuss how to implement the Knowledge Database within an enterprise. Some companies, for example, have already employed incident management solutions that provide pre-installed repository capabilities. It is also possible to create a webpage/portal that is connected to the SQL database on the company's server.

G: Disclosure strategy mapping.

After referencing to the Knowledge Database, the team will have enough retrieved information to solve the disclosure puzzle, and decide on an optimal incident disclosure strategy. It would be wise to run the framework with a list of possible cyber security incident scenarios to determine which information is required for the database. This paper presents an example of the minimum required information, such as applicable legal requirements, a company's stakeholders with up-to-date contact information, and incident disclosure templates.

H: The Incident Status Updates.

It is important to keep in mind that when the IRT is deciding on the disclosure strategy, the information about the incident may change. For example, it can be later discovered that the compromised server actually stores personal data, though there was no such information during the incident impact assessment and filling in the incident questionnaire. In this case, it is important to receive the incident status updates, e.g. from IT analysts or engineers, during the mapping process in order to quickly re-adjust the strategy.

Fourth step. Post-disclosure learning

The framework allows a company to start learning from its disclosure activities. Once there are clear disclosure procedures in place, the learning opportunities become feasible. The disclosure report might be generated on every incident with the list of decisions regarding the disclosure audience, timeline, content, and methods. If a company operates across multiple locations, and there is a similar attack on the systems in, for example, the Netherlands, as it was in Germany a month ago, it would be very beneficial to check how the IRT from Germany performed in that case.

Therefore, the final and fourth step in the flowchart refers to learning activities from the incident. After the disclosure strategy has been developed (I), it should be confirmed that the notifications were made according to the strategy, and if not, why not (J). Then, the IRT team can summarize the lessons learned from the particular disclosure approach (K), that together with incident details and disclosure steps will be filed and stored at the Knowledge Database (L).

VI. Validation

The proposed framework has been validated in three ways. Due to space limitations, we here only sketch some highlights related to this. The first test of our framework was to show that it does address all identified challenges from the four categories "To whom", "When", "What", and "How". To do so, we matched the challenges identified in section III and analyzed whether the framework truly covers them all. The result of this analysis is shown in Table II of the appendix. It lists all the challenges together with explanations how the framework can help in solving each issue. The column *Framework solution* shows what framework tools are being used in order to obtain information required to resolve each challenge.

A second validation step was executed by defining two security incident scenarios. The aim was to check the feasibility of the framework and to understand in more detail how the flowchart processes work. The discussed incident scenarios made clear how the framework automates the decision-making around incident disclosure issues. It turned out from the examples that the framework utility and efficacy heavily rely on the content of the knowledge database. For more details on this validation step, we refer to [32].

A third validation step was done by interviewing a group of experts. This helped us understand what advantages and difficulties can be associated with the implementation of the framework in the company. If adopted, the major change the framework is supposed to make to the business world is that it contributes to automating the process of decision-making regarding incident disclosure (while, currently, most of the companies still rely on group discussions during incident response meetings). Still, the framework value may vary depending on the industry, since it depends on the scope and the complexity of the environment a company operates in, and hence the amount of information it needs to make a final decision. For many more details on this validation step, we here again refer to [32].

VII. Conclusions

In this paper, we started by identifying a basic set of factors that influence the organizational preferences regarding incident information disclosure and combined these with four different strategy questions to create an overview of all disclosure challenges involved in cyber security incident response. Based on that, the aimed incident disclosure framework could be designed. The resulting framework was presented in section V.

The framework in a nutshell is a decision support tool that automates and facilitates the process of making disclosure decisions during the meetings of a security incident management team. Using the framework will not produce a concrete disclosure strategy, but it will provide necessary information from the database that matches incident details as well as organizational priorities regarding incident disclosure in a specific situation. This information will help the team to develop a specific incident disclosure approach.

The introduced framework tools, such as Incident Specifics Questionnaire and Incident Response Priorities, hasten the process of developing an incident disclosure strategy without affecting the quality of final decisions. The framework is not organization-specific, but it establishes a baseline from which any company can easily adjust the framework to its operational settings and business needs.

By providing a clear step-by-step guide to follow, the framework motivates companies to a more structured approach in their incident response procedures. For example, the framework can push organizations to make a detailed elaboration of roles and responsibilities within teams dealing with cyber security incidents. That will ensure that every framework process has its owner and remains under control.

Overall, the framework provides a more intelligent approach to cyber security incident response, by allowing companies to decide faster with whom, when, how, and what to share without losing the quality of decisions. That in turn will cause positive spillover effects on external audiences that will receive timely and content-wise information, and thus will perform actions that are beneficial to society as a whole.

References

[1] W. T. Coombs and S. J. Holladay, *The Handbook of Crisis Communication*: John Wiley & Sons, 2012.

[2] B. Reynolds and M. W. Seeger, "Crisis and Emergency Risk Communication as an Integrative Model," *Journal of Health Communication,* vol. 10, pp. 43-55, February 2005.

[3] M. Hossain and H. Hammami, "Voluntary disclosure in the annual reports of an emerging country: The case of Qatar," *Advances in Accounting,* vol. 25, pp. 255 - 265, 2009.

[4] Verizon. (2012). *2012 Data Breach Investigations Report*. Available: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[5] RSA. (2011). *A New Era of Compliance. Raising the Bar for Organisations Worldwide.* Available: http://www.rsa.com/innovation/docs/CISO_RPT_1010.pdf

[6] R. L. Dilenschneider and R. C. Hyde, "Crisis communications: Planning for the unplanned," *Business Horizons,* vol. 28, pp. 35 - 38, 1985.

[7] M. Smith, R. Hunter, and K. McGee, "Opportunities and Threats in a World of Great Transperency," Gartner, September 2010.

[8] Internet Security Alliance (ISA) and t. A. N. S. I. (ANSI). (2010). *The Financial Management of Cyber Risk*. Available: http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf

[9] J. B. Kaufmann and I. F. Kesner, "The myth of full disclosure: A look at organizational communications during crises.," *Business Horizons,* vol. 37, p. 29, 1994.

[10] G. K. Meek, C. B. Roberts, and S. J. Gray, "Factors Influencing Voluntary Annual Report Disclosures By U.S., U.K. and Continental European Multinational Corporations," *Journal of International Business Studies,* vol. 26, pp. 555-572, 1995.

[11] P. M. Healy, A. P. Hutton, and K. G. Palepu, "Stock Performance and Intermediation Changes Surrounding Sustained Increases in Disclosure*," *Contemporary Accounting Research,* vol. 16, pp. 485-520, 1999.

[12] W. T. Coombs, "Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory," *Corp Reputation Rev,* vol. 10, pp. 163-176, 2007.

[13] P. M. Schwartz and E. J. Janger, "Notification of Data Security Breaches," ed: Michigan Law Review, Vol. 105, p. 913, 2007.

[14] H. Khurana, J. Basney, M. Bakht, M. Freemon, V. Welch, and R. Butler, "Palantir: a framework for collaborative incident response and investigation," presented at the Proceedings of the 8th Symposium on Identity and Trust on the Internet, Gaithersburg, Maryland, 2009.

[15] K. M. Moriarty, "Incident Coordination," *Security Privacy, IEEE,* vol. 9, pp. 71 -75, nov.-dec. 2011.

[16] S. Romanosky, R. Telang, and R. Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis and Management,* pp. 256-286, 2011.

[17] K. Hausken, "Information sharing among firms and cyber attacks," *Journal of Accounting and Public Policy,* vol. 26, pp. 639 - 688, 2007.

[18] K. R. Fitzpatrick and M. S. Rubin, "Public relations vs. legal strategies in organizational crisis decisions," *Public Relations Review,* vol. 21, pp. 21 - 33, 1995.

[19] L. Ponemon Institute. (2011). *2010 Annual Study. Global Cost of a Data Breach*. Available: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon

[20] D. M. Dekker, C. Karsberg, and B. Daskala. (2012). *Cyber Incident Reporting in the EU. An overview of security articles in EU legislation*. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu/at_download/fullReport

[21] NYSE. (2003). *Final NYSE. Corporate Governance Rules*. Available: http://www.nyse.com/pdfs/finalcorpgovrules.pdf

[22] the Division of Corporation Finance of the U.S. Securities and Exchange Commission (SEC), "CF Disclosure Guidance: Topic No. 2 - Cybersecurity," ed, 2011.

[23] R. Kalb. (2012). *Disclosures 2012: Level of cyber-security risk disclosures varies after new SEC guidance*. Available: http://blogs.reuters.com/financial-regulatory-forum/2012/04/06/disclosures-2012-level-of-cyber-security-risk-disclosures-varies-after-new-sec-guidance/

[24] D. S. Alberts and R. E. Hayes, *Power to the Edge: Command and Control in the Information Age (Information Age Transformation Series)*: CCRP Publish Series, 2003.

[25] C. E. Carroll, *Corporate Reputation and the News Media: Agenda-Setting Within Business News Coverage in Developed, Emerging, and Frontier Markets (Google eBook)*: Taylor & Francis, 2010.

[26] PWC. (2011). *Cybercrime: protecting against the growing threat. Global Economic Crime Survey*. Available: http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf

[27] PWC. (2011). *Cyber crisis management: A bold approach to a bold and shadowy nemesis*. Available: http://www.pwc.com/en_US/us/forensic-services/publications/assets/cyber-crisis-management.pdf

[28] P. Argenti. (2011). *Digital Strategies for Powerful Corporate Communications*. Available: http://www.europeanfinancialreview.com/?p=2581

[29] M. J. G. van Eeten and J. M. Bauer, "Economics of Malware: Security Decisions, Incentives and Externalities," OECD Publishing, OECD Science, Technology and Industry Working Papers, May 2008.

[30] E. Van Ruitenbeek, *The Common Misuse Scoring System (CMSS) [electronic resource] : metrics for software feature misuse vulnerabilities / Elizabeth Van Ruitenbeek, Karen Scarfone*. Gaithersburg, MD :: U.S. Dept. of Commerce, National Institute of Standards and Technology, 2009.

[31] R. McMillan, "Six Decisions You Must Make to Prepare for a Security Incident," Gartner, September 2011.

[32] O. Kulikova, "Cyber Crisis Management, a decision-support framework for disclosing security incident information," TBM, Delft University of Technology, Delft, 2012.

TABLE II. FRAMEWORK SOLUTION FOR THE IDENTIFIED CHALLENGES.

Category	**Challenge**	**Framework solution**
Harm mitigation and prevention		
"To Whom"	Identifying the right stakeholders to be informed for effective incident response and harm mitigation	Incident impact assessment (to determine initial notification stakeholders) + the Questionnaire + stakeholders contacts from the Database (to clarify additional internal and external stakeholders)
"When"	Identifying when to release notifications to facilitate the incident response process	the Questionnaire (to clarify the incident details) + Priority Sliders (to adjust the notification timeline)
"What"	Creating a proper notice to each stakeholder group, so they can evaluate risks and take the right course of actions	the Questionnaire (to clarify the incident details) + notice templates and stakeholder groups from the Database
"How"	Identifying notification methods that assure speed and correctness of the disclosed information	the Questionnaire (to clarify the incident details) + communication policy from the Database + location specific communication channels from the Database
Regulation		
"To Whom"	Identifying who must be notified due to legal requirements, if any	the Questionnaire (to clarify the incident details) + location specific disclosure regulations from the Database
"When"	Identifying the specific timings of stakeholders notification required by law, if any	the Questionnaire (to clarify the incident details) + location specific disclosure regulations from the Database
"What"	Identifying what information must be in the notice due to legal requirements, if any	the Questionnaire (to clarify the incident details) + location specific disclosure regulations from the Database
"How"	Identifying what notification methods to use due to legal requirements, if any	the Questionnaire (to clarify the incident details) + location specific disclosure regulations from the Database
Cost-efficiency		
"To Whom"	Assuring that the scope of notified audiences reflect the severity of the incident	Incident impact assessment (to assign the initial group of stakeholders that reflects incident severity) + the Questionnaire + stakeholders contacts from the Database (to clarify additional internal and external stakeholders)
"When"	Assuring that the disclosure times do not further aggravate a company's situation	the Questionnaire (to clarify the incident details) + Priority Sliders (to adjust the notification timeline) + disclosure recommendations on "when" from the Database (as an advice)
"What"	Assuring that information disclosed does not create further financial losses	the Questionnaire (to clarify the incident details) + Priority Sliders (to determine the company's external disclosure posture) + disclosure recommendations on "what" from the Database (as an advice)
"How"	Identifying cost-efficient notification methods	the Questionnaire (to clarify the incident details) + location specific information on communication channels
Reputation		
"To Whom"	Identifying stakeholders who can help restore reputation, and those who can damage it	the Questionnaire (to clarify the incident details) + Priority Sliders (to set the focus on reputation) + stakeholders contacts from the Database matching the incident details and related to reputational issues
"When"	Identifying the appropriate timings of incident notifications that is beneficial for a company's reputation	the Questionnaire (to clarify the incident details) + Priority Sliders (to adjust the notification timeline) + disclosure recommendations on "when" from the Database
"What"	Identifying what disclosure content can help restore reputation, and do not damage it	the Questionnaire (to clarify the incident details) + Priority Sliders (to set the focus on reputation) + disclosure recommendations on "what" from the Database
"How"	Identifying notification methods that are beneficial for a company's reputation	the Questionnaire (to clarify the incident details) + Priority Sliders (to set the focus on reputation) + disclosure recommendations on how" from the Database