CYBER CRISIS MANAGEMENT:
A DECISION-SUPPORT FRAMEWORK FOR DISCLOSING SECURITY INCIDENT INFORMATION

by OLGA KULIKOVA

July 12, 2012

Master Thesis

CYBER CRISIS MANAGEMENT: A DECISION-SUPPORT FRAMEWORK FOR DISCLOSING SECURITY INCIDENT INFORMATION

by

OLGA KULIKOVA
Student number 4122151
kulikova.o.j@gmail.com

Committee:

Dr.ir. Jan van den Berg, First Supervisor
Associate Professor at ICT section

Dr.ir. Wolter Pieters, Second Supervisor
Information security researcher at Energy&Industry

Prof. Dr. Y. H. Tan, Chair
Head of ICT section

Ronald Heil, External Supervisor
Senior Manager at KPMG IT Advisory

Master Programme Management of Technology
Faculty of Technology, Policy, and Management
TU Delft

July 12, 2012
DELFT

Dedicated to my dearest mom and dad.
Without your love and support, I would have never made it this far.

ABSTRACT

The growing sophistication and frequency of cyber attacks, as well as the impossibility to completely secure IT systems force modern companies to be prepared beforehand for cyber security incidents and data leaks. An advanced cyber attack can easily trigger a crisis that involves numerous internal and external stakeholders. The way a company disseminates security incident information among them is an essential part of incident mitigation. A proper incident disclosure strategy can significantly improve the timeliness and the effectiveness of incident response activities, while a poor strategy can lead to legal penalties and costly lawsuits. Incident information disclosure, hence, is becoming an important issue that requires good internal procedures in place to facilitate incident response process and do not cause further damage for a company and its audiences.

In this research project we determined four dimensions that shape organizational preferences regarding incident information disclosure: harm mitigation and prevention, regulatory compliance, cost-efficiency, and reputation. Together, they create challenges for a company when deciding to whom, when, what, and how share incident information. After a thorough examination of existing recommendations on the incident disclosure and business needs, we developed a decision-support framework that provides step-by-step guidance for organizations on developing an appropriate incident disclosure strategy. The overall validity and reliability of the developed framework was tested using cyber incident scenarios and through an interview with a security expert.

The proposed framework provides structure to enable incident disclosure processes within a company, and, at the same time, it gives flexibility to customize the framework according to organizational business needs. The framework can be applied to all kinds of security incidents, but its main focus is on dealing with incidents of a cyber security nature. It incorporates strategic and tactical advice found in the literature, as well as organizational preferences and concerns regarding the incident disclosure discovered through the interviews. The framework broadens a pure technical, "wall-and-fortress" approach to manage cyber security incidents. It increases company's chances to successfully mitigate the consequences of such incidents and get the business quickly back on track.

ACKNOWLEDGMENTS

This research has given me an invaluable opportunity to meet and work with a lot of highly inspirational and professional people.

I would like to express my sincere gratitude and appreciation to my TU Delft supervisors: dr.ir. Jan van den Berg and dr.ir. Wolter Pieters for their great mentorship and advice that provided guidance and direction for my thesis research. Your constructive criticisms, suggestions and encouragement sharpened my research skills and enhanced my writing experience.

I would also like to thank my KPMG supervisor, Ronald Heil, whose advice and suggestions enriched my knowledge and helped me better understand how the real world works. Thank you for your positive influence in growing my vision.

A great part of my gratitude goes to everyone from the ISC team of KPMG. My internship turned out to be an amazing learning experience in such a friendly and yet highly professional environment. Marek, special thanks to you for giving the valuable comments on my framework design, and the overall support during the internship. Jeroen, thank you for your contribution to our little stagiairs team: it was fun (except one shooting episode).

I would also like to thank all the interview participants who made this research possible by contributing their valuable time and expertise.

Finally, I want to thank my family and friends. You have all inspired me, helped me stay focused, and finish my research.

Marcus, Kristian, Tony, Bassem, Paul, Elliot, many thanks for proofreading this report.

– Olga Kulikova
Amstelveen, June 26, 2012

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

He who tries to defend everything defends nothing.

— Frederick II, Holy Roman Emperor

My idea, in its entirety, is that if vile people unite and constitute a force, then decent people are obliged to do likewise; just that.

— Leo Tolstoy

1.1 BACKGROUND AND MOTIVATION

Even the casual observer could have noticed the recent uproar over cyber attacks on governments and businesses worldwide. "Cyberwar Is Already Upon Us" or "A Digital Pearl Harbor Is Only a Matter of Time" are just a few headline examples of recent hot discussions over cybersecurity. The magnitude and impact of cyber attacks have been rising significantly over the past decade, capturing widespread public attention and involving in discussion not only corporations and cyber specialists, but also media, politicians, and the general public. In 2012, cyber attacks are among the top five global risks in terms of likelihood [1], clearly becoming one of the major concerns for developed societies.

"...Technology and the Internet confer great advantage on attackers. The cost, effort and risk to the attacker are low, the reward is high, and the targets are all in one place - the Internet." [2]

Most enterprise systems nowadays rely on computer infrastructures - whether in storing, processing, and transferring data, or controlling and monitoring physical processes. It is a big dynamic domain where an enormous amount of innovation is going on; thousands of tools and applications are being developed on an ongoing basis to help companies in their needs. All these technologies have multiple points of vulnerabilities which give adversaries various opportunities to disrupt and paralyze IT systems or steal valuable information they contain [3].

Different research studies have found that companies usually view cybersecurity as a technological task and focus on investing in mainly technical solutions to defense against cyber attacks, like employing intrusion detection systems (IDS) or log analysis [4, 5]. The reality is, however, that cyber criminals are constantly improving in their targeting and approach at a speed which for many organizations is almost impossible to match [6]. Recently, Bloomberg Government conducted a study with 172 organizations in different industries and found that organizations *"would need to increase their cybersecurity spending almost nine times over – to $46.6 billion from the current $5.3 billion – to achieve security that could repel 95% of known attacks."* [7] Obviously, organiza-

"There are two types of companies: those who know they have been attacked, and those who don't." FBI Director Robert Mueller.

tions cannot afford such spendings to guarantee total security, so in the end, organizations are not only attacked often, but also attacked successfully [8, 6].

A new challenge has emerged for modern enterprises - shifting the organizational focus of dealing with cyber incidents from pure technology centric to processes and stakeholders centric, in order to get a better handle on cyber incidents [9, 10]. Cybersecurity is no longer a technical discipline, it has evolved into a strategic concept, where effective incident management procedures have to be established to help companies reduce as much as possible harm caused by serious cyber attacks [11].

It has long been acknowledged that an essential part of effective incident management is *communication with stakeholders*, since it can facilitate incident response process, assure compliance, and influence external perceptions about the company [12, 13, 14]. During the process of mitigating the impact of an incident and possibly finding its causes, various parties need to be properly informed such as infrastructure or application providers, third-parties, or business representatives [15, 5]. In addition, countries worldwide are introducing regulations that require organizations to disclose certain incidents to such audiences like affected individuals, government agencies, or law enforcement [16, 17, 18]. Finally, keeping external parties informed about the incident response process can help a company to influence its brand image damaged after the incident.

There are, however, certain disincentives for companies to disclose security incident information, such as fear of bad publicity, costly legal actions, or revealing too much data on their cybersecurity efforts. A fear of losing a good reputation becomes another disclosure barrier, since admitting a mistake could lead to loss of customers and negative public scrutiny in general. However, a company that decides not to share relevant information bears a significant risk that affected stakeholders would know about data leak from third parties or cyber attackers themselves. In this case, the consequences can be much worse, like a complete loss of clients' confidence or civil and criminal penalties for failure to report cybersecurity incidents. Complex interconnections between people involved in security incidents, as well as changes in responsibilities during crises when the higher management takes over certain roles, make the situation even more difficult.

A good 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 contrast, a bad incident disclosure strategy can lead to legal penalties and costly lawsuits, and cause further harm to affected parties [16, 4]. Incident information disclosure is becoming an important, complex issue that requires good internal procedures in place to fa-

cilitate incident response process and do not cause further harm for a company and its audiences.

1.2 RESEARCH GOAL

Decision-making considerations described in the previous section eventually form a big question for modern companies on how to create procedures for effective notification of stakeholders after a cyber attack. There is a critical need for a decision support framework that will ensure incident information disclosure to internal and external stakeholders in line with both organizational goals and existing requirements. This framework should give an answer on *when, what, how,* and, most importantly, *to whom* to disclose incident information, within a company as well as outside it, to effectively mitigate the consequences of a cyber security incident.

The goal of this thesis research is defined as follows:

> *To design a decision-support framework on organizational disclosure of cyber security incident information to internal and external stakeholders that facilitates incident response in line with organizational goals and existing requirements.*

Such framework would provide a step-by-step guidance for an organization on accessing the situation and finding the best solutions on how, what, when, and to whom disclose cyber security incident information.

In order to gain a profound understanding of the problem environment and in-depth knowledge on current business goals and challenges, the following subquestions should be addressed prior to a framework development:

Q1 Why is cybersecurity a problem for modern organizations?

Q2 What challenges do organizations face when deciding on their incident disclosure strategies?

Q3 What recommendations are given in literature on effective notification of external and internal stakeholders?

Q4 How does a real company perform cyber security incident management regarding information disclosure? What are the main preferences and concerns?

Q5 What should be the process of arriving at a disclosure strategy taking into account information gathered from previous questions?

1.3 RESEARCH STRATEGY

This master thesis is based on the Design Science research approach[1], in detail elaborated by Hevner et al. A design science project is a set of nested problems in which the top level problem is always a *practical* problem. The main question of this research is a practical problem on designing an organizational decision-support framework, which is decomposed into set of knowledge subproblems (Q1-Q4) and practical subproblems (Q5), introduced in the previous section.

This research is conducted in the following phases that are aimed at answering the identified subquestions:

1. *Problem conceptualization (Q1).* In this phase the study focus is established. We discuss challenges cyber attacks poses for modern enterprises, describes cyber adversaries and their tools, and consequences of successful attacks. We show that proper incident information disclosure to internal and external stakeholders is becoming an important task for modern organizations in their incident response activities.

2. *Problem analysis (Q2).* In this phase we assess the current situation within organizations and identify challenges they are facing when deciding on incident disclosure strategies. These challenges help to define what should a good decision-support framework deal with.

3. *Synthesis of Practice-Oriented Theories (Q3).* In this phase we summarize major recommendations on incident information disclosure from scientific articles and industry white papers with respect to identified challenge categories. These recommendations are integrated in the framework design to assure rigor of the study.

4. *Comprehension of Business Needs (Q4).* In this phase we gain insight in the current "state-of-the-art" of incident information disclosure. Results from semi-structured interviews are presented and critically examined in order to acquire a thorough understanding of business needs regarding incident information disclosure. These requirements are addressed by the framework to assure the research relevance.

5. *Development stage (Q5).* Here, we design the decision-support framework on cyber incident information disclosure in accordance with the acquired understanding of the business needs and synthesized knowledge.

1 A detail explanation of the Design Science research method can be found in Appendix A.

6. *Evaluation stage (Q5).* Here, we evaluate the framework by using cyber security incident scenarios and by asking for a security expert opinion. Findings are relevant for future improvements of the framework design. They also set new research opportunities regarding cyber security incident disclosure.

1.4 THESIS STRUCTURE

The thesis structure is aligned with the main research phases, as shown at Figure 1.

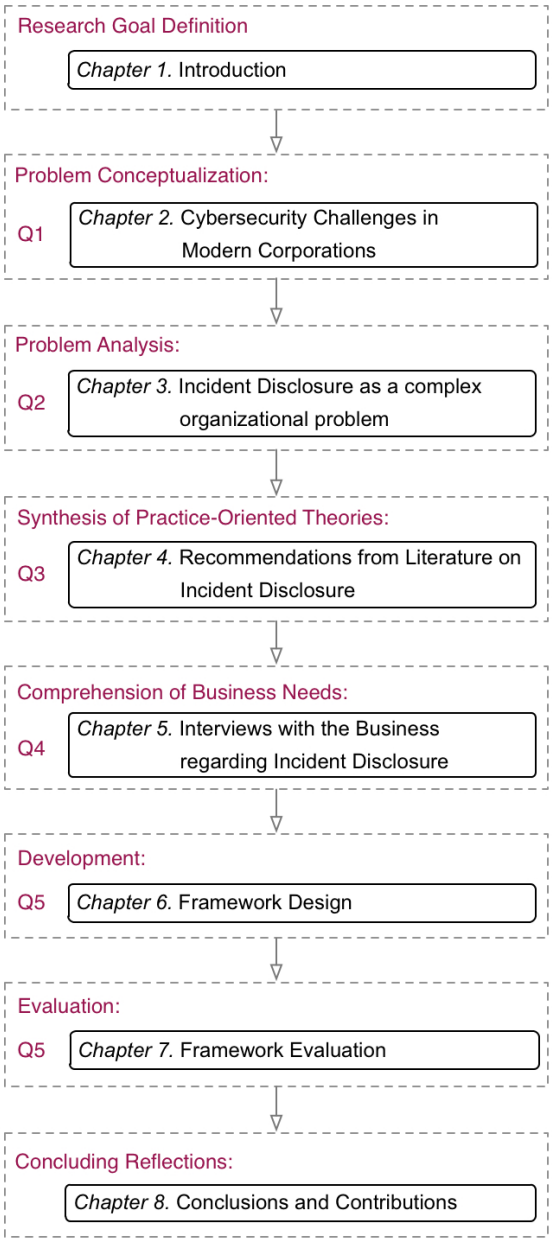


Figure 1: Thesis Outline

2

CYBERSECURITY CHALLENGES IN MODERN CORPORATIONS

2.1 WHY CYBERSECURITY?

We live in a world where enterprises worldwide have their critical databases connected to the Internet or rely on computer systems that monitor and control their operational processes. These business realities create a target rich environment for cyber attackers across the globe [20]. Some attackers are interested purely in money, others in exposing or paralyzing business operations of corporations and government agencies [6, 21]. The range of cyber adversaries varies from teen hackers to organized crime groups, industrial spies, terrorists, and even governments [22, 21].

Despite an attacker's identity or motivation, a successful intrusion could cost a company a lot of trouble - financial losses, data leaks, business disruptions, or infrastructure failures [22]. The global market is becoming more and more interconnected, with new stakeholders joining every day, meaning that a cyber attack on one company could easily trigger unexpected negative events in others [23]. Keeping information and operations secure, thus, is of vital importance for any enterprise, which becomes the task of *cybersecurity*.

2.1.1 *Key Definitions*

In this research, we refer to cybersecurity as *body of technologies, processes and practices designed to protect organizational networks, computers, programs and data from attack, damage or unauthorized access* [24]. Or, by using information security attributes, cybersecurity seeks to ensure *confidentiality*, *availability*, and *integrity* of digital information and information systems [25, 26].

When a company experiences negative cybersecurity events like data breaches, systems interruptions, malware, or virus outbreaks, it can be referred to as a *cyber incident*. The precise definition of a cyber incident depends on a particular company. However, in broader terms, we can talk about an adverse event in an informational or operational system that impose harm or the attempt to harm for an organization [27].

There could be different causes of cyber incidents. Natural disasters, like Hurricane Katrina, can create a cyber incident by turning off electrical supply of an organization and thus shutting down their IT systems [28]. In this case, it is said that the cause of an incident

is *unintentional*. This master thesis, though, looks at cyber incidents that are *intentional* and caused by *cyber attacks* - deliberate human attempts to evade security services and violate the security policy of a system [27].

It is important to understand what kind of challenges cyber attacks create for modern companies. Being fully aware of who represents the cyber threat, what they can do and what can be an impact of a cyber intrusion is the first step of any organization in designing their incident response procedures [22, 21]. The remaining part of this chapter is aimed at answering these questions.

2.2 GETTING REAL ABOUT CYBER ADVERSARIES

As long as information technologies exist, there have always been individuals or groups that use it inappropriately for different reasons. At starters it was mainly recreational hackers who liked to make some technology-based jokes or intrude in networks just for fun or showing off. It was random activity, that did not target specific companies. Hackers were not intending to cause harm to other computers, and some of them even developed and followed a hacker's ethics [29].

However, the changing ways of doing business have created new opportunities for people with criminal intentions. When computers and networks became inevitable part of corporations, when large amount of credit card numbers, account credentials, and other valuable information became reachable through the Internet, hackers realized that they could make money on it and began to organize criminal groups [29, 5]. Through online message boards, they have started to share intrusion techniques and newly discovered vulnerabilities reducing the marginal cost of cyber crime [6, 30]. Less technical skill have become required to take advantage of the organizational networks. Before the world knew it, cyber crime became a global activity, with the participants from all over the world communicating anonymously.

The situation is getting worse. Nowadays money is not anymore the main purpose of cyber attacks. The rich variety of information being stored on organizational servers and different tools available to perform intrusions have allowed cyber adversaries to experiment with final attack goals. Besides, more and more operational technologies, like SCADA, are becoming accessible from the Internet and thus potentially vulnerable to assault. Cyber attacks are being used for espionage, industrial sabotage, or even as a sort of punishment for organizations who are doing business in a way not appreciated by hacker communities. Attacks stopped being random, today's many hackers know exactly whom they want to strike and are patiently waiting for the results [21, 23].

2.2.1 *Who are they?*

In general, the current literature on cyber threats distinguish the following groups of cyber adversaries [31, 22, 23]:

INDIVIDUAL HACKERS
: Individuals who are making unauthorized attempts to bypass the security mechanisms of organizational informational and operational systems for their own specific purpose. They can be either insiders (disgruntled employees) or outsiders (individual phishers, spammers, malware authors).

INDUSTRIAL SPIES
: Individuals or groups spying to obtain secret information for commercial purposes, for example on science and technology. The goals of cyber espionage can vary from saving money on research and development to undercutting a competitor's tender.

ORGANIZED CRIME GROUPS
: Groups that use computer systems and the Internet as the main element to create fraud, such as distribution of malware, phishing, and theft of valuable information such as credit card credentials. In the majority of cases, the goal is economic fraud, where there is an intention to steal money, property, or a legal right.

HACKTIVISTS
: Hacktivists are hackers who perform attacks for a politically or socially motivated purpose [5]. Actions of hacktivists are not aimed at individuals, but rather companies or government entities with an attempt to cause disruptions to their networks and services in order to bring public attention to some political or social cause. Quite often referred to as white hats since their main goal is not to commit crime but "to expose the corruption and greed inherent in the playbooks of big business and rogue regimes powered by hyper-capitalism and intent on plundering the natural resources of the planet." [32]

NATIONAL GOVERNMENTS
: Governments that initiate state-sponsored espionage, for example for national security purposes, or deliberately perform sabotage in other countries as part of some political operation.

TERRORISTS
: Terrorist groups that moved to cyberspace with an intention to use computer, networks, and public internet to cause destruction and harm for political or ideological objectives.

2.2.2 *What are they after?*

"If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without shooting a single bullet." [33]

No longer is it the time when cyber attacks are targeting financial institutions and agencies operating with personal information that can be stolen. Nowadays cyber attacks can also target operational industries like water, oil and gas sector, since these systems are more and more controlled using computing equipment that is connected to the Internet. The Stuxnet attack on the Iranian plant, for example, has become a wake-up call for the modern world, proving that critical infrastructures are also exposed to cyber attacks [11]. At this moment, the governmental concern about cyber attacks is becoming more understandable. While hacking commercial enterprises was being seen as mainly their internal problem, attacks against control systems and critical infrastructures are extremely undesirable for societies as a whole.

The recent study on purposes of cyber attacks revealed that intrusions to disrupt business and production processes happened more often than other ones [21]:

1. Disruption of business and production processes - 30,0%;
2. Access to money - 16,6%;
3. Obtaining information on intellectual property - 16,1%;
4. Access to third party information or systems - 14,6%;
5. Obtaining Information concerning business operations, e.g. mergers and acquisitions - 12,1%;
6. Others - 10,6%.

It is crucial to discover which company's assets can be exploited by cyber attackers, not only from financial point of view, but keeping in mind other attackers motivations. Security specialists mention the following goals of cyber adversaries as a check-list for an enterprise [22, 21, 23]:

- personal interests (showing off, revenge),
- financial interests (theft, business competition),
- intellectual property interests (espionage),
- ideological interests (political disagreement),
- state interests (policy makers decisions, military strategies).

There is also a growing tendency in *multi-stage attacks*, when cyber adversaries target a company just because it is in the middle of some value chain, and can be used as a bridge to exploit other organizations [16]. Hence, a company's assessment of potential cyber attacks goals should also cover important players in its value chain.

2.2.3 *What are their tools?*

Today's Internet gives a perfect opportunity to collaborate and exchange tools for criminal activity through social network platforms and file exchange websites. As a consequence, cyber attacks are becoming more standardized, automated, and easier to perform. Eventually, more sophisticated intrusions can be performed by less mature adversaries [9].

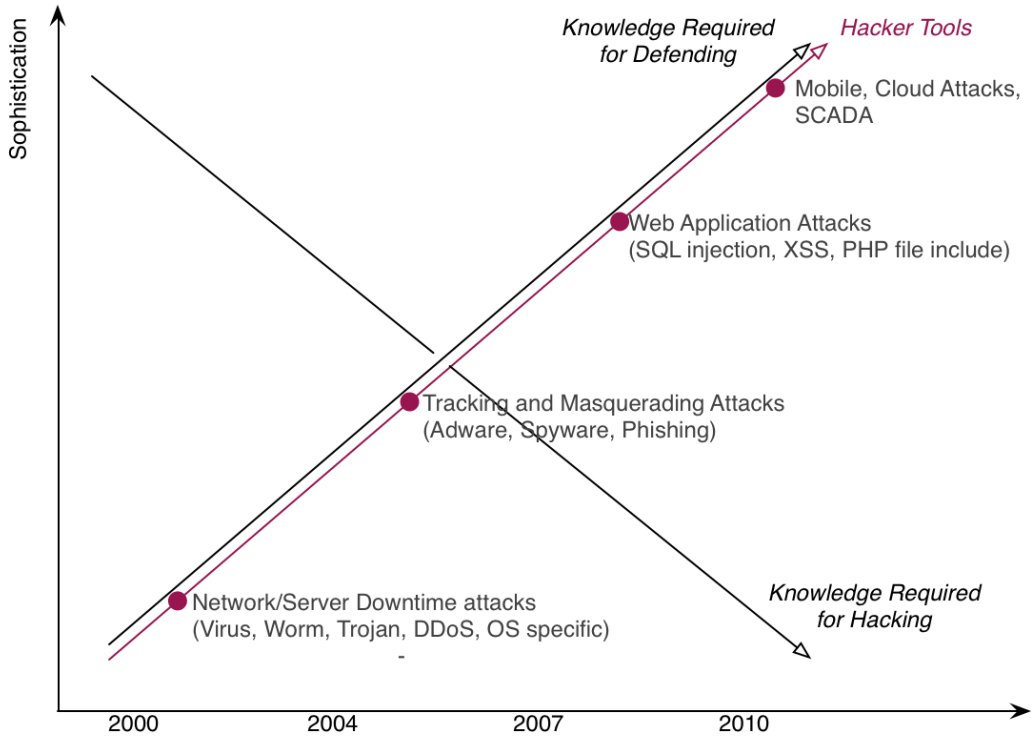


Figure 2: Ever changing threat landscape. Adapted from Walk.

Figure 2 illustrates the sophistication of hacking knowledge through the past decade and lists the most common tools to perform attacks. New attack vectors have appeared, as well as the types of virus payload. It all started with attacks on personal computers, and now mobile devices and cloud computing are in the game as new ways of storing enterprises information. Organizations have to consider all possible types of cyber attacks, so significant technical knowledge is required to combat them, in contrast to the knowledge required for hacking.

In addition to the general sophistication of hacking tools, attacks nature have also changed from *traditional* to *advanced* once. Robert Lentz, the CEO of Cyber Security Strategies, clearly explains the shift in his *Cyber Security Maturity Model* [35]. According to him, cyber attacks used to be openly known, exploiting known unpatched vulnera-

bilities, targeting a broad range of people and organizations, and only for one-time hit. In recent years attacks have become more *stealthy*, exploiting *zero-day vulnerabilities*, *targeting* specific organizations, and *persistent* by nature (Figure 3). Such attacks are also commonly known as *Advanced Persistent Threats (APT)*.

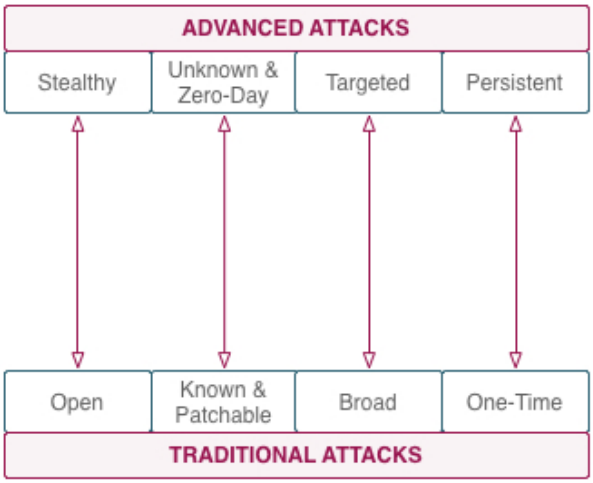


Figure 3: A shift towards advanced cyber attacks. Derived from Lentz [35]

APTs can easily create severe consequences for an organization, involving multiple stakeholders, and requiring high-level incident response strategy in order to minimize damage and quickly resume mission essential functionality.

2.3 DEFENSE AGAINST CYBER CRIME. SHIFTING PERSPECTIVE

"Notwithstanding rapidly growing investments in security measures, it has become clear that cybersecurity is a technological arms race that, for the immediate future, no one can win." [?]

The trends described above shift the overall perspective of how to defend against cyber adversaries. The World Economic Forum report on Global Risks of 2012 [1] emphasizes it by introducing *Axioms for the Cyber Age*:

1. Any device with software-defined behavior can be tricked into doing things its creators did not intend.
2. Any device connected to a network of any sort, in any way, can be compromised by an external party. Many such compromises have not yet been detected.

In other words, the traditional "wall-and-fortress" approach, like installing firewalls and anti-viruses, is not enough anymore to keep intruders out, and cyber incidents will happen. This fact is recognized by the majority of security specialists, but still remains a big challenge for companies that want to change their methods in dealing with cyber attacks and develop strategies that will help them limit the damage.

2.3.1 *Cyber Security Maturity Model*

Lentz, former chief security officer of U.S. Department of Defense, in his *Cyber Security Maturity Model* measures the state of cybersecurity governmental and private companies by introducing five levels of maturity on the way towards resilience against cyber attacks [35] . The model places the majority of modern companies at Level D - when technologies are at the core of responding to cyber threats (Figure 4). These companies are close to combating traditional cyber threats, but there is still long way to go to defend against the APTs.

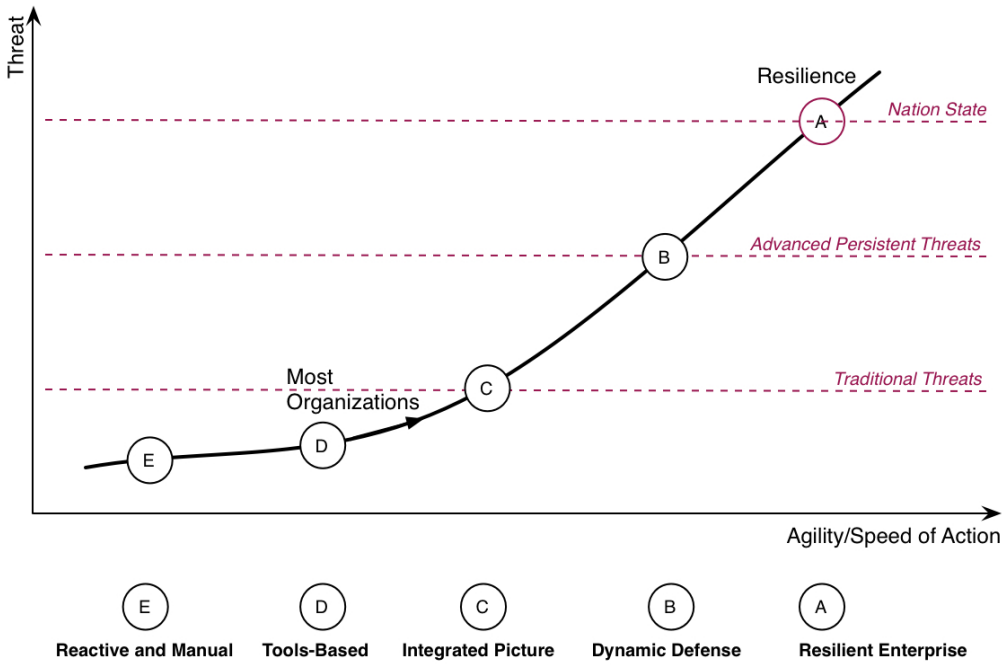


Figure 4: Cyber Security Maturity Model. Derived from Lentz [35]

A. RESILIENT ENTERPRISE
: Predictive and mission focused, the enterprise isolates and contains damage, secure supply chains and protect key critical infrastructures to operate through cyber attack;

B. DYNAMIC DEFENSE
: Predictive and agile, the enterprise instantiates policy, illuminates events and helps the operators find, fix, and target for response;

C. INTEGRATED PICTURE
: Loosely integrated with focus on interoperability and standards based data exchange for situational awareness;

D. TOOLS-BASED
A company applies tools and technologies to assist people in reacting faster to cyber incidents;

E. REACTIVE & MANUAL
People based following doctrine and doing their best to "put out fires".

2.3.2 *Cyber Crisis Management Solution*

In order to combat APTs and reach the level B on the curve, treating cyber incidents only as a technical problem is not longer a solution for modern enterprises. The scope and nature of cyber attacks have changed, as well as the amount of public attention surrounding them. A company will have to develop an entire cyber crisis management solution that will assure agility and overall effectiveness of incident mitigation.

PwC [5] introduces the main stages of the cyber crisis management shown in Figure 5. Only some of the stages require technical resources, like ongoing threat monitoring, or root cause analysis. Others, such as law enforcement coordination, public relations and media, breach notification, require right policies and people in place to ensure effectiveness of cyber crisis management.

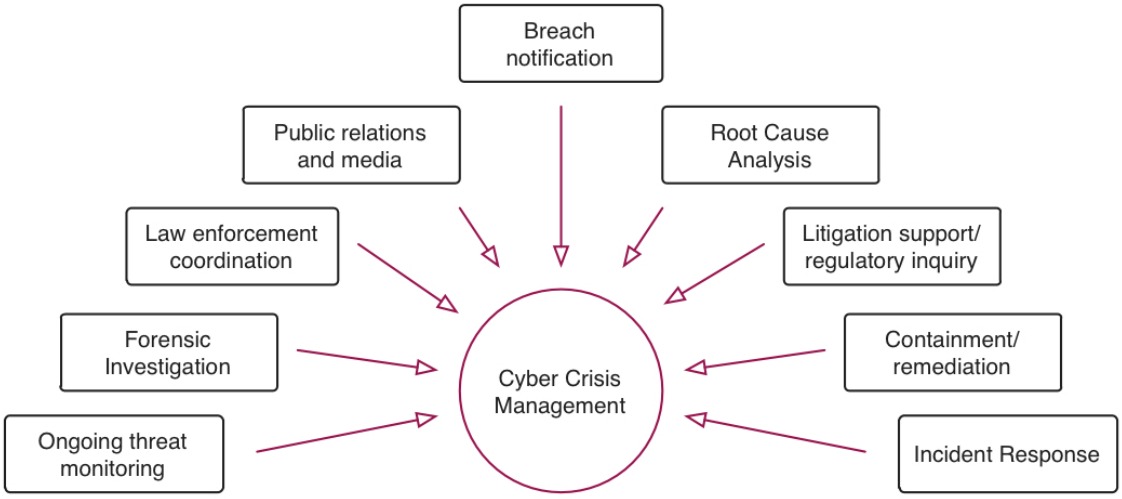


Figure 5: Cyber Crisis Management Process. Derived from [5]

Having organizational services in place, related to public relations, breach notifications, or communication with third-parties like law enforcement, would broaden pure technical approach to managing cyber security incidents. By ensuring coordinated messaging among all parties involved, a structured response can be guaranteed to increase a company's chances of successfully mitigating the harm and get the

business quickly back on track. It is an essential step for any company that wants to increase their level of cyber security maturity.

2.4 SUMMARY

In this chapter we showed how the task of cybersecurity has slowly become one of the main concerns for modern enterprises. We revealed the nature of cyber adversaries, what their motives are, tools, and what damage they can create for an organization by initiating cyber attacks.

While many cyber attacks can be relatively harmless (not doing any evident damage to equipment or systems, or targeting data that well encrypted), some of them, like APTs, may easily lead to a crisis situation to be managed. For instance, when there is a leak of personal data or disruption of services. We discussed why, especially in case of advanced attacks, incident response is no longer a pure technical problem, and requires policies and people in place to guarantee structured cyber crisis management.

Coordinated messaging, or information disclosure, between key audiences was shown as an important part of cyber crisis management. The next step is to determine more precisely how a company can benefit through a proper incident information disclosure strategy, and what should be done in order to guarantee its effectiveness during the incident response process.

3

INCIDENT DISLOSURE AS A COMPLEX ORGANIZATIONAL PROBLEM

In the previous chapter we showed that the current state of cybersecurity means that organizations hardly have a chance to withstand all cyber attacks, especially the advanced ones, and therefore cyber incidents, unfortunately, will occur. Already several decades ago researchers agreed that incidents cannot be planned, but a company's *response* to them *can* be "in enough scope and detail to minimize damage of a potentially explosive situation." [14] As part of incident management, incident information disclosure to stakeholders has been widely considered as the cornerstone activity during a crisis as it can have a significant impact on the timeliness and effectiveness of incident mitigation [36]. A lot of research has been done on discovering the role of information disclosure in incident management procedures, its benefits, drawbacks, and the challenges a company faces when developing their disclosure strategies [12, 37, 38, 39].

The challenge of this research is that, despite the rich literature base on crisis communications, only a few papers specifically target cybersecurity crisis situations [5, 4, 16]. The vast majority discusses the issue from a broader perspective, not going into details of incident types that might affect a company. While some general findings and advice can still be applicable to cyber incidents, this research aims to look at incident information disclosure not only from a general perspective, but also to take into account specifics of cybersecurity incidents.

3.1 DISCLOSURE DEFINIED

At this point it is important to define more precisely the term *disclosure*. During this research "disclosure" will be used as a shorthand for the dissemination of cyber security incident information to internal and external stakeholders.

Incident information disclosure is the key element of *crisis communications* and should not be confused with it. Crisis communication is a broader field which also includes such activities as the collection and processing of incident information [37].

Such terms as *"information dissemination"*, and *"stakeholders notification"* will serve as synonyms to "disclosure" and appear periodically in the report.

3.2 WHY PLAN FOR INCIDENT DISCLOSURE?

Every crisis creates the need for information, both for people dealing with it inside the company as well as outside audiences [37]. Incident information disclosure, thus, is an essential part of crisis communications, which can, according to Reynolds and Seeger "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." [39] 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" [40].

Speaking about cyber incidents, in 2011, 92% of cyber security breaches are discovered by a third party [9], 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 [16].

"The consequences of any unplanned-for occurrence, however calamitous, can always be less costly, and less traumatic when 'crisis communications' are thoughtfully prepared in advance." [14]

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 [14]. In contrast, clear communications can help to quickly engage internal and external stakeholders in incident response, and help them make sound decisions faster [41]. It will increase overall transparency of an organization, which is beneficial for any company in times of new disclosure regulations and increased public scrutiny [41]. An information disclosure plan would guarantee the described benefits and limit the chance of further incident escalation.

3.3 INTERNAL AND EXTERNAL STAKEHOLDERS. WHO ARE THEY?

Being complex by nature, cyber incidents involve various internal and external stakeholders, which further complicates crisis management activities. Since these stakeholders constitute the objects of disclosure, it must be clearly understood who are the stakeholders among which, if cyber attack occurs, information should be disseminated.

While the precise set of stakeholders depends on the particular case, a company still can distinguish general groups of stakeholders

depending on their motives and capabilities. McMillan from *Gartner Research* introduces four major incident response stakeholders (Figure 6):

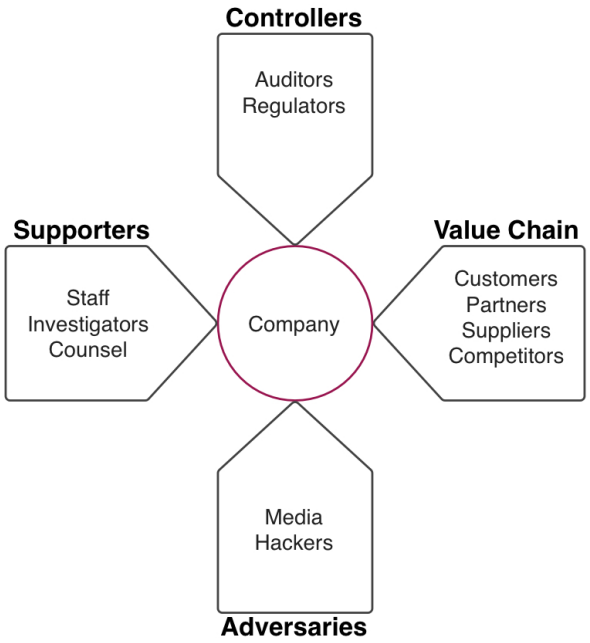


Figure 6: Incident Response Stakeholders. Derived from [42]

CONTROLLERS
- entities that ensure a company meets standards in dealing with cyber incidents;

SUPPORTERS
- entities that help a company to respond to a cyber attack;

VALUE CHAIN
- entities that are core to the business;

ADVERSARIES
- entities that may work against a company.

Each stakeholder group may require different notification in terms of time, content, and methods. The value chain wants to be quickly and fully informed of the impact of a cyber incident on business. Controllers require other piece of information - that disclosure proceeds in accordance with requirements and does not impede investigations. Supporters, if notified earlier and in greater technical detail, can assist greatly in responding to an incident. Even maintaining communication with adversaries, as been said in "keep your friends close, and your enemies closer", can help a company to suffer less damage from media coverage and possible further attacks from cyber adversaries.

In general, 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 supporters, or restoring reputation in the eyes of the value chain and media [4, 38, 16]. 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.

3.4 FOUR DIMENSIONS OF INCIDENT INFORMATION DISLOSURE

The first step in solving the described decision-making puzzle is to look inside the black box of a company's behavior and define the main *dimensions* that shape organizational preferences regarding when, what, how, and with whom to share security incident information. Trying to satisfy the requirements of all dimensions, a company faces various challenges to deal with (introduced later in Section 3.5) in order to choose the most appropriate incident disclosure strategy.

To get a better understanding of the organizational determinants to disclose security incidents, we investigated the available literature regarding information disclosure. Meek et al. state that 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" [43]. Public pressures from media and reputational concerns are mentioned by Healy et al. and Coombs as another determinant of organizational disclosure strategy. In general, these claims correlate with the findings of Schwartz and Janger, who, in their research on data breach notifications, conclude that organizational disclosure strategies are influenced by three forces: *regulatory, economic, and reputational.*

These authors, however, does not consider the process of incident response itself as a motivation to disclose security incident information. Still, 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 [46, 47]. Cyber incidents are becoming more sophisticated and frequent. Companies lack employees that can deal with the whole scope of potential security attacks. In this case, information sharing among companies and government agencies on security incidents can become a "life saver" in case of advanced cyber attacks [47, 4].

As a consequence, in this research we add the fourth determinant *harm mitigation and prevention* to the three ones previously identified by Schwartz and Janger. Eventually, it gives us four determinants (or "dimensions", as we refer in this research) of security incident

information disclosure: *harm mitigation and prevention, regulatory compliance, cost-efficiency,* and *reputation* (Figure 7). We chose the name "cost-efficiency" rather then "economic" to get a better representation of what is meant by this dimension - ensuring that the perceived benefits of the disclosure exceed the perceived costs.

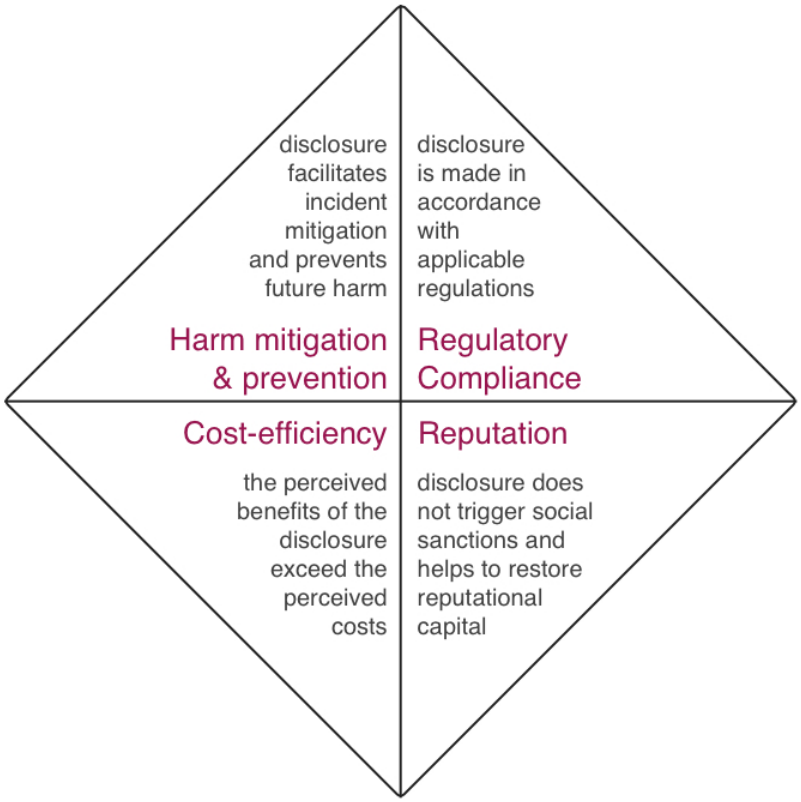


Figure 7: Four Dimensions of Cyber Incident Information Disclosure

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.

3.4.1 *Harm mitigation and prevention*

When a crisis strikes, time to make decisions is short, available information is limited, and overall pressure is high. The role of human decision-maker becomes a crucial one [45], which requires timely and relevant information to be disseminated across an organization in order to make sound decisions. Incident information disclosure, thus, becomes a cornerstone activity in harm mitigation after a security incident. It can reduce the chance of incident escalation and limit its interference with normal business operations.

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 [48]. 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 cybersecurity [45, 47]. Hausken, in his paper on information sharing among firms and cyber attacks, showed that organizational aggregate defense can be improved through exchange of information with other companies, when security investments become too costly [49].

While being a necessary activity within a company, incident information disclosure to outside audiences can be quite dangerous and cause even more harm. It can attract new waves of hackers trying to exploit the publicly announced vulnerabilities, thus escalating an incident. Or it can make criminals engage in fraud, who will pretend to provide help for affected stakeholders. As a consequence, a fear of providing cyber attackers with the "roadmap" inside the company or causing further damage to stakeholders often prevents firms from sharing the data on cyber security incidents.

Last but not the least, organizations may already have individuals who are responsible for a wide range of activities regarding cyber security. Still, there is neither standardized job descriptions which determine responsibilities of each position, nor proper description of how communication channels should be organized between employees and with external stakeholders [50, 45]. Incident disclosure strategy should address this problem, so a cyber security harm can be effectively mitigated and the risk of future harm can be reduced.

3.4.2 *Regulatory compliance*

Regulatory compliance can prevail in the organizational decision - making process during a crisis, also with respect to incident information disclosure [13]. Recent cyber attacks on DigiNotar [51] and KPN [52], and the delays with which dependent stakeholders were informed of the data breaches, show that companies are still lacking a good approach on stakeholders notification. In order to address the issue, 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 [53].

Currently, the requirements on disclosure of cyber security incident information exist when 1) there is leak of personal data; 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 [16]. These regulations require that notification 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. Regulations set the costs highest for the high-risk breach types, and cyber attacks are among them. 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* [1] for every listed company on the New York Stock Exchange (NYSE) [54]. Before last year, companies used to exclude cyber incidents from the scope of SEC requirement since it did not explicitly state otherwise. To clarify the situation, SEC issued guidance on October 13, 2011, which emphasizes that cyber-risks should be disclosed as any other type of incident [55]. Since then, a company has to determine the correct definition of what constitutes a material cyber security incident and disclose them in financial statements, annual reports, or Forms 10-K, 20-F, 40-F [18].

What further complicates the regulatory compliance in terms of incident disclosure, is that cyber transactions are not tied to particular location as laws usually are [4]. 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." [16] 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. Please refer to Appendix B for a detailed problem example and a list of data breach notification laws around the globe.

1 Event is considered *material* if it can influence investment decisions of the company's investors. Or, simply say, if an event impacts the company's stock price, then it is material.

3.4.3 *Cost-efficiency*

Financial resources is the main determinant of an organizational choice of their disclosure strategy [12]. According to Schwartz and Janger "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 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 may even create so-called *disclosure disincentive*: a company will prefer to stay silent if there is no external discovery of an incident [45]. It will allow avoiding costly legal actions and dedicating organizational resources and time to actual incident response, instead of dealing with media, law enforcement, and other agencies. Additionally, public disclosure of an incident can indirectly benefit a company's competitor, when old customers or investors will decide to switch to the competitor in order to feel more secure.

With respect to cyber security attacks it might be expected that the quick notification of affected parties is in the company's best interest. However, according to the *Ponemon Institute's* annual investigation [53], 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 [56], and how to determine these "timely" frames is becoming a big issue, to assure both cost-efficiency and safety of the company's reputation.

3.4.4 *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, 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 [57].

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 [53]. According to a recent survey from *PwC*, reputational damage is the biggest fear of 40% of respondents when experiencing cybersecurity incidents [8].

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 [5, 12]. 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 [57]. 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 [45]. At the same time, if a cyber incident is discovered externally (which happens quite often, as mentioned earlier), no matter how much a company wants to keep quiet, as Argenti fairly notices: *Silence... can prove to be a brand's most damaging strategy."* [58].

A company may also chose a different disclosure strategy in terms of crisis justification. Cyber attacks are performed by people with malicious intents, so a company may opt for posing as a victim, and defense against any negative feedback by blaming hackers. Or, if an incident is the result of a simple attack which the company could have prevented by having better security controls, and external audiences know it, a company would rather apologize and ensure that it has learned from the incident.

3.5 CYBER INCIDENT DISCLOSURE CHALLENGES

The four described dimensions create a situation during a crisis when a firm's ability to quickly access the situation and arrive on the appropriate disclosure approach becomes limited at best.A company starts facign decision problems regarding the audience and timing of notifications, the notification content and methods of information disclosure. Below, in Table 1, we summarized challenges from the four dimensions into the following categories:

"WHOM" category applies to audience receiving incident information notifications. It can be any party out of the four stakeholder groups introduced earlier: value-chain, supporters, controllers, or adversaries.

"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. A notice may include the issue time, the senders, the receivers, the subject, and the main body [59].

"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-mails, phones, website postings, newspapers, television, etc.

	"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 reflect 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 do not damage it	Identifying notification methods that are beneficial for a company's reputation

Table 1: Incident Information Disclosure Challenges

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.

3.6 SUMMARY

In this chapter, we discussed why planning for disclosure is important for any company as well as defined stakeholder groups that fall

under the scope of notifications. We introduced the four key dimensions of incident information disclosure strategy that determine a company's preferences on what, when, how, and with whom to share after a cyber crisis strikes. In examples, we showed how these dimensions create notification alternatives for a company to choose from. These choices result in a set of challenges for a company to deal with, which are summarized in the table in the last part of the chapter.

Every incident is unique, and there will never be a silver bullet among disclosure strategies that will solve every disclosure problem a company faces. Still, if a company employs certain procedures and tools that help in analyzing all of its choices, there is a good chance that the final disclosure strategy will bring the best possible outcome. The decision-support framework, hence, must employ certain mechanisms that will allow a company to find a solution for each of the identified challenges from the table.

The next step is to collect all relevant recommendations from theory and practice that address the introduced decision challenges. These recommendations will be necessary to provide a solid base for the decision-support framework; to ensure that it is built upon an existing knowledge base and considers the current business needs regarding incident information disclosure.

4

RECOMMENDATIONS ON CYBER INCIDENT INFORMATION DISCLOSURE, A LITERATURE REVIEW

Having identified organizational challenges on cyber incident information disclosure, the next step is to review current academic and professional literature that may give useful recommendations on how to deal with the described problems. Such review is essential for this project to guarantee that the final outcome is built upon existing knowledge and that the working advice have been taking into account.

An important starting point is that *there is no commonly agreed strategy on incident information disclosure.* It is true for any type of incident, not only cyber related. Every incident has a unique set of traits [4], plus different organizations follow different business models [30], 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 [45, 38, 4].

To have a generic disclosure plan is the first and very important step in a company's efforts to build effective communications, but a company must have some decision-making support mechanism that will help to adjust this plan for every crisis situation. This mechanism should assist in dealing with every challenge category we introduced earlier.

In this chapter, we discuss two common types of recommendations on crisis communications, and summarize advice related to all identified challenge categories: disclosure audience, time, content, and methods. In the end, we gather the major recommendations in one table, to incorporate them later in the framework design.

4.1 STRATEGIC VS. TACTICAL ADVICE

What we noticed during the literature review, is that, in general, there are two different approaches to giving recommendations. Some authors and security firms go with a narrow look at the problem and provide a set of "how to" instructions, like *"prepare for follow-on inquiries by opening a 1-800-xxx call center"* [60, 4]. Other authors look at the problem of crisis communications from a broader perspective, by giving recommendations that are particularly designed to help organizations achieve certain business goals [37, 36, 39]. One example can be a full-disclosure strategy to help a company restore its reputation [38].

Coombs explains this situation by dividing crisis communication theory into *tactical* and *strategic advice*. According to him, "strategic crisis communication research seeks to understand how crisis communication can be used to achieve specific outcomes and have the desired effect on stakeholders." [61] In contrast, tactical advice is more about performing concrete actions, so a certain strategy can be accomplished. Tactical advice can vary widely for different types of industries, different locations, and type of data a company operates with.

We find this double nature of advice as a good approach to collect the recommendations from the literature on the identified challenge categories. Further sections will present advice from the literature based on their strategic or tactical nature.

4.2 RECOMMENDATIONS ON AUDIENCE TO WHOM INFORMATION IS DISCLOSED. "TO WHOM"

4.2.1 *Strategic advice*

With respect to *internal* notifications, the main goal a company pursues with its disclosure strategy is harm mitigation after a cyber incident, so there should be a clear process established for gathering the incident response group on a very short notice [5]. The roles and responsibilities of people joining the team should be well defined, that vary depending on the level of the incident [4]. An incident level is established during the incident impact assessment, when a company estimates the overall impact they experience because of the incident [62].

With respect to *external* notifications, the situation is more complicated by specifics of every incident and the mix of goals a company wants to accomplish with their disclosure strategy. In some cases, like personal data leaks, a company could set the regulatory compliance as the first preference and immediately notify law enforcement or government agencies to avoid possible legal fines in future [45, 16, 4]. In case of an advanced cyber incident, a company may decide first to notify third-parties with cyber experience, asking them for assistance in the incident response and harm mitigation.

Trying to deal with this variety of options, several authors introduced a strategy that describes two main levels, or thresholds, that trigger notifications to specific audiences such as external authorities or affected individuals. Burdon et al. call this strategy *two-tier notification trigger approach*. The first threshold concerns security incidents resulting in unauthorized access and data acquisition, but there is no evidence of harm to external audiences. The second threshold concerns incidents with the reasonable risk of harm, like criminal misuse

of data [63, 45]. Depending on the threshold, a company is advised to notify the following external stakeholders:

the 1st threshold. Acquisition trigger
: Notifications to a designated regulatory authority only. It will give the company a chance to postpone extensive notification duties and focus instead on incident investigation and response activities.

the 2nd threshold. Risk-based trigger
: Notifications to all affected individuals and other relevant authorities. Regulatory compliance will become dominant in the disclosure strategy and require proactive actions in notification of all required by law parties.

For the second threshold, a company may also consider including media and public contacts in its notification list. If external audiences were affected by an incident, it will trigger "aggressive 24/7 media attention" [4, 57]. For a company that cares about its reputation, communications with media would become a decision priority in order to protect or restore its reputational capital. Some authors suggest to release media announcements only after consulting with law enforcement or legal authority, to make sure that disclosure itself does not violate any legal requirements or impede the incident investigation [45, 4].

Voluntary incident information sharing

In addition, a company may find it beneficial to voluntary share information on cyber incidents with various third-parties - across the value chain, with competitors, agencies for protecting critical infrastructures, and country created exchange platforms, like Information Sharing and Analysis Centers (ISACs)[1]. The following benefits can be named:

- trigger united incident response together with other companies;
- optimize organizational cyber crisis management based on the received feedback;
- increase global cyber defense by sharing security solutions among companies, law enforcement, and other industry groups;
- using benefits of public-private partnerships (PPPs[2]) in combating cybercrime;

1 The goal of ISACs is to share valuable cybersecurity information among their members. Several ISACs have been formed for industry sectors such as Communications, Electric Sector, Financial Services, Information Technology, and Research and Education[64]

2 PPPs allow to use the knowledge of both private and public companies in order to improve the defense against cyber criminals. The Netherlands is the pioneer in

4.2.2 *Tactical advice*

Tactical recommendations regarding whom to notify internally are mainly focused on making the company prepared beforehand for the security incident. A company should have a pre-defined list of employees who will compose the incident response team depending on the impact level of the incident [4, 64]. Furthermore, a company should have a list of employees, who will join the team during the incident response depending on the specific details of the incident. For instance, if the incident was discovered externally, and the general public is already aware about it, involving a social media coordinator would be an essential step for the company to reduce the negative public mood.

With respect to possible external disclosures, companies are advised to have an up-to-date list of external contacts, for immediate access if needed. For example, a company may consider hiring an outside counsel with extensive experience in legal requirements in case of personal data breaches. The counsel will assist in clarifying requirements of notifications, and also bring more opportunities for a company to comply with laws of multiple jurisdictions by having access to a global legal network.

A company may also consider hiring an external organization that specializes in crisis communication during the incident response. Any crisis puts a lot of pressure and stress on staff, so external supervising can help a company to maintain a "cool head" and do not make mistakes in its notification efforts [5].

The third parties, which are involved in the company's business operations and were affected by the incident, should be contacted as well in order to prepare for future inquiries from the stakeholders. For example, if there was a big data leak on the credit card account details, the company should notify a bank that issued these credit cards as soon as possible, so it can be ready for information requests from the affected individuals.

4.3 RECOMMENDATIONS ON CONTENT OF WHAT IS BEING DISCLOSED. "WHAT"

4.3.1 *Strategic advice*

Content of notifications reflects organizational explanation and justification for the crisis. A firm may employ a reputation restoring strategy, and take responsibility for a crisis by including apology in

the field and currently has law enforcement, private security firms, consultants and academia involved in PPPs. Together they manage to take down the Bredolab botnetwork that involved 143 servers associated with the botnet, gaining international attention due to their collaborative efforts [21].

the notifications to external stakeholders, or focus on harm mitigation, and deny responsibility by providing only objective information about the incident [12]. Coombs summarizes crisis communication strategies regarding what a company may say to external parties during the crisis:

- *Attack the accuser.* A company confronts the person or group claiming that the organization experiences a certain incident;
- *Denial.* A company states that there is no incident;
- *Scapegoat.* A company blames external parties for what happened[3];
- *Excuse.* A company denies intent to do harm and claims inability to control the events that triggered crisis;
- *Justification.* A company acknowledges the incident and minimizes the perceived damage caused by the incident;
- *Compensation.* A company states that affected stakeholders will be compensated;
- *Apology.* A company claims full responsibility for the incident and asks stakeholders for forgiveness;

A firm also needs to decide on the amount of information to release. It can disclose incident information *fully, partly, or not disclose it at all*. Each approach has its drawbacks and benefits, and the goal is to find the optimal level of disclosure. Kaufmann and Kesner in their paper on full disclosure suggest the following questions, or "checklist", to determine the amount of information to disclose:

1. Could non-disclosure lead to further injury?
2. Is an organization the culprit or the victim? (e. g., bad security controls in place vs. extensive DDoS attack on the website)
3. Are the fictions surrounding the crisis worse than facts?
4. Can an organization afford to disclose? (Does it have enough money to engage in lawsuits later?)
5. Can an organization afford not to disclose? (Is there a good chance that silence will not cause significant harm for a company?)

For example, if a company sees that sooner or later an incident will be discovered externally, and seriousness of this incident is high, it can go with a full disclosure strategy called *"Stealing thunder"* - when

3 Quite popular strategy in case of cyber attacks - a firm blames hackers, and not its bad security controls

a company itself breaks the news about crisis, before it is discovered by the media or other parties. This is perceived as a good strategy for a company to enhance its credibility and trustworthiness, and make crisis look less severe in the eyes of the outside world. Recommended for the companies who want to be forgiven for its role in the incident.

Overall, a disclosure policy should consider the described checklist to help managers ask the right questions while deciding on the amount of information to disclose. The list can be adjusted with the new questions, depending on the company's nature. The key is to always maintain flexibility and make notifications that reflect the crisis situation.

4.3.2 *Tactical advice*

Any advice on the exact content of notifications would be of a tactical nature, since information to include in every notice is very incident specific. The foremost thing to remember regarding the notification content, according to many specialists [4, 45, 15], is that different types of stakeholders require different notice. It is advisable to have a pre-defined message templates for each stakeholder group for different incident scenarios. Chandler suggests to create message mapping database, that will contain templates of messages for different stakeholders groups for different types of security incident that can occur in the organization, as shown at Table 2.

Incident	Incident Stage	Topic	Audience	Notification Method	Message Template
Personal data leak	Management	Update on steps to investigate the breach and mitigate losses	Customers	First-class mail and web announcement	...
...	...	...	Staff	...	
			Third-parties		
			Media		
			Regulators		
			...		

Table 2: Message Mapping Template. Adapted from [15]

The notice should be written in clear, concise and easy-to-understand language to avoid misunderstandings and wrong actions from stakeholders. Example information to include in the notice that is addressed to affected parties can be found in Appendix C

4.4 RECOMMENDATIONS ON TIME WHEN INFORMATION IS DISCLOSED. "WHEN"

4.4.1 *Strategic advice*

Internal notification timeline follows the company's communication policy, and must assure that a crisis response group is organized a soon as possible after an incident confirmed. New and emerging issues during the incident response process should be communicated to responsible personnel not later than the minimum time interval set out by the company's communication plan [4].

The external notification timeline is adjusted on a case-by-case basis with the first check on whether mandatory deadlines for notification exist due to legal requirements. This will guarantee getting regulatory compliance under control. Some papers specifically state 48 hours as the maximum delay for the first round of notifications, if there are external stakeholders affected by an incident. After the "legal" timeframes are checked, a company may decide to issue external announcements only in response to media inquiries concerning an incident, but until that stay quite. Or, a company can initiate an incident communication on its own prior to any external publications on the incident, for example if it is a culprit of an incident, and there is a low chance to hide what happened.

In general, the following key considerations on timeliness and frequency of information release to external parties are mentioned in the literature [38, 4, 12]:

- whether a notice would disrupt an ongoing investigation process (e.g. by Europol chasing a hacker);
- whether a notice would create public distrust and panic with consequential irrational decisions due to an early announcement;
- whether a notice would create a notification fatigue and public ignorance due to high frequency of public announcements;
- whether a notice would lead to extra fines due to a bad chain of custody maintenance (e. g., for very quick notices);
- whether an early notice would help to prevent reputational loss.

4.4.2 *Tactical advice*

Various stages of crisis will dictate different notifications to key stakeholders, so notifications should be mapped in time for each stage. A typical crisis has six stages, according to Chandler: *warning*, *risk*

assessment, response, management, resolution, and recovery. As in the previous section it is encouraged to map notifications to the stage of an incident by using a message mapping database (Table 2).

Security specialists suggest not to notify customers prematurely, until a company has all the information about the incident. Facts continue to appear, and the additional round of notifications with different or even opposite information is highly undesirable, since it costs money and creates further problems for the company's credibility and reputation. Besides, a company may become a subject of legal fines due to false or inaccurate announcements [5, 60].

4.5 RECOMMENDATIONS ON METHODS BY WHICH INFORMATION IS DISCLOSED. "HOW"

4.5.1 *Strategic advice*

Regarding the methods of notifications both to internal and external stakeholders, the main strategic advice is that a company should always evaluate the crisis situation and use such communication channels that will not only provide compliance, but also assist in incident mitigation and prevent further harm.

For example, if there is a high media attention to the crisis, a company may find it insufficient to have only one contact person, even if "one" guarantees better control over the information that leaves the organizational walls. Media can start contacting different people in the organization. So instead of referring all the questions to one single person, a company would better make a list of most possible contacted people, and make sure that they are constantly updated on the status of the incident [65]. It will prevent from inaccurate information leaving the company and all follow-up negative consequences.

Another advice is to have all tools available that will assure timeliness and correctness of transmitted information [64]. The complete list of "must-have" communication tools can be found in Appendix D.

4.5.2 *Tactical advice*

The most advisable method of notifications is postal mail, in case a company is sure that contact details of its stakeholders are correct. If postal mail notification is too costly (e. g.an incident affected a big number of individuals), or contact information is outdated, substitute means of notice like media public announcement, or website posting can be used. Email notifications quite often are not advisable, since individuals can treat them as "phishing" emails [60, 4].

Finally, a company must be prepared for follow-on inquiries and establish two-way communication, by opening 24/7 call center with the toll-free number [60].

4.6 RECOMMENDATIONS SUMMARY

Our goal is to integrate the strategic and tactical recommendations described in the previous sections in the decision-support framework. Therefore, it is important to give a clear summarization of the recommendations, in order to simplify the process of the framework development. Table 3 recaps the major findings of the chapter. Later, it will be shown how the framework addresses every advice from the table in its design.

	Strategic advice	*Tactical advice*
"To whom"	— The incident response team is informed prior to any other notifications. Its composition reflects the impact level of the incident.	— Create a pre-defined list of employees with their contact information that are involved in the incident depending on its impact level.
	— Different notification triggers to certain stakeholders depending on the incident result (e.g. unauthorized access, theft or misuse of data, or systems disruptions).	— Create a pre-defined list of employees with their contact information that will further join the incident response team based on the incident specific details
	— Regulations check once the incident is confirmed, on the required notification audience.	— Create and update the contacts of external counsel as well as companies specialized in crisis communications and incident response.
	— Voluntary sharing as a possible harm-mitigation or reputation restoring tool.	— Create and update the contact information of third parties that might be involved in the security incident.
"When"	— Notifications timeline adjustment depending on the legal requirements, incident details, and organizational priorities in the incident response.	— Try to avoid early public notifications, before all the information is available about the incident. If delays are not possible, incident status update should be established to quickly re-adjust the disclosure strategy.
"What"	— Content and the amount of information to release reflects the incident details - a company's role in a crisis (culprit, victim), incident discovery (internal, external), legal requirements, etc.	— Create and maintain message mapping database with different notification templates related to different stakeholder groups, types of security incident, or incident stage
"How"	— Communication channels should be chosen in accordance with the incident details (e.g. wider public attention leads to a stronger reliance on social media channels like Twitter)	— Create and maintain the list of the preferred notification methods depending on the location specifics, affected stakeholders, and regulation requirements (postal mail, emails, phone calls, etc).

Table 3: Strategic and Tactical Advice on the Incident Information Disclosure

4.7 SUMMARY

This chapter provided an overview on currently existent recommendations related to crisis communications and incident information disclosure. There is a little attention to cyber incidents disclosure in

academia papers. They are more concerned about crisis communications in general, and provide mainly strategic advice. Recommendations that are particularly related to cyber crisis management were found in papers of security organizations, and they are more tactical in nature. We see the need to effectively combine two fields: crisis communications together with specifics of cyber crisis management; and two types of advice: strategic and tactical, in the later framework design.

We did not come across any cyber incident disclosure framework that would provide clear steps for a company to develop their disclosure strategies. The main reason could be, as we said earlier, the very specific nature of every cyber incident and every business operations.

At this moment we have the first half of information required for the design science research - the knowledge base obtained from the literature to assure rigor of the study. The next step is to understand the current business needs and see how a real company performs security incident disclosure, internally as well as externally, with respect to the four identified dimensions. This information, integrated in the framework design, will ensure the research relevance.

5 INTERVIEWS

The previous chapter elaborated on existing recommendations regarding incident information disclosure found in the scientific literature as well as industry white-papers. Now, the goal is to understand "state-of-the-art" within an industry that relies in their operations on computer systems and thus becomes a subject of cyber incidents. For this purpose, a series of field interviews was conducted with a large company that pays close attention to its cybersecurity posture, to get a better understanding of current business needs regarding security incident communications.

5.1 THE TARGET COMPANY

The idea was to find a company that treats cybersecurity as a high priority, since it would give a better chance that the company looks beyond technical solutions in response to cyber incidents and is interested in implementation of security policies and procedures that will facilitate an effective incident response. We wanted to interview a company that already had experienced problems related to cyber incident disclosure with respect to four dimensions: harm mitigation, regulatory compliance, cost-efficiency, and reputation.

The choice fell on a large oil refinery company[1] that is interested in the implementation of better security incident disclosure mechanisms. The oil industry is highly regulated, so there is an opportunity to discuss regulatory compliance issues. The industrial processes of oil and gas themselves requires high level protection from any cyber adversaries, as their attacks can lead to very destructive consequences, so the company does take into account the problem of harm mitigation and prevention. Cost-efficiency is typically at the core of any business strategy, so there should be some room for discussion as well. Finally, being a large company widely known in many countries, it should take into account reputational issues when developing its communication strategies.

5.2 APPROACH

The interviews were conducted with the following employees as shown at Figure 8:

- a compliance coordinator with knowledge on legal issues;

1 For security reasons, the company's name cannot be disclosed in this research.

- a coordinator from incident response team who is involved in the actual incident response process;
- a surveillance coordinator who is involved in increasing organizational awareness of the current state of IT and the threats across the globe, to reduce the possibility of incidents in the future;
- a coordinator from the incident response management (IRM) team with knowledge on strategic preferences of the company regarding incident communication;

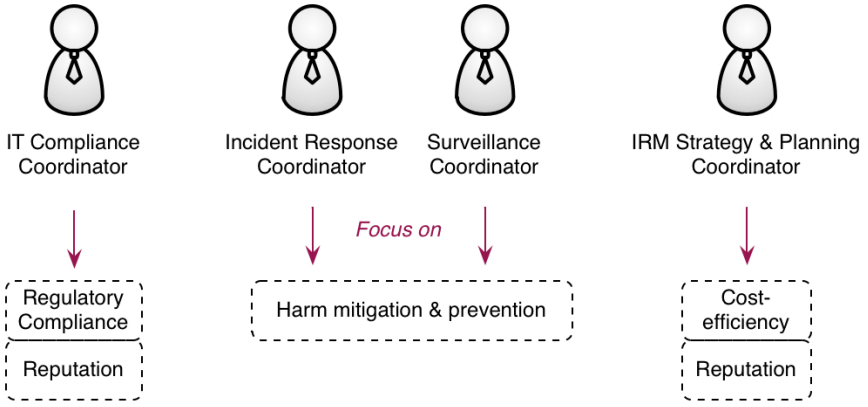


Figure 8: Interview Approach

By ensuring that all four coordinators participate in the interviews, this research is able to draw conclusions about decision-making regarding all four dimensions of the incident information disclosure.

The interviews were planned as semi-structured, with a short introduction in the beginning for better understanding of the coordinators positions within the company. A short list of standardized questions was developed to initiate a conversation; the list can be found in Appendix E. Later, depending on the answers, we could continue with open questions, trying to find specific details and nuances of the incident management process, with respect to communication and information disclosure procedures. Questions were developed with the goal in mind to clarify how the company currently deals with cyber incident information disclosure and mark out its main preferences and concerns. They cover internal and external notifications, what problems the company faces along the way, what are the advantages of the current procedures, and what can be improved.

5.3 KEY FINDINGS

5.3.1 *Overview*

1. *Internal notifications are based on the incident impact level discovered through the Business Impact Assessment;*

   The company has already put internal procedures in place for notifying internal personnel in case of a security incident. The Escalation and Communication procedure defines internal stakeholders to be notified depending on the Class of an incident after business impact assessment[2] (BIA). BIA considers financial, operational, customer, and employee-related losses, which also includes damage to the company's reputation. There are three possible classes of an incident: Class 3 refers to low impact incidents, Class 2 refers to medium impact incidents, and Class 1 refers to high impact incidents. Every incident class has a predefined set of employees to notify immediately after the incident is confirmed. Still, since every incident is unique, specific employees are invited to join an incident response team on a case-by-case basis. Decisions on how, when, what, and who to notify are determined throughout the incident response meeting. Currently, there is no knowledge database that can assist in answering these questions.

2. *Unified approach to all kinds of security incidents;*

   The majority of coordinators find this internal notification procedure quite effective. It is a unified response approach to all kinds of security incidents including cyber ones, so people do not get confused by having several options on what to do. One coordinator, though, noted that perhaps some cyber incidents, like the compromise of an email account of a high-level executive, could not be evaluated according to the described procedure, and thus it may be difficult to assign the proper personnel to handle the case.

3. *No procedures established for external notifications;*

   At the moment there are no procedures in place for notifying external stakeholders. The members of the incident response team make decisions case-by-case after consulting with the legal expert, who participates in every discussion to make sure that all decisions have a legal basis.

4. *Difficult to learn from the previous disclosure strategies.*

2 When it comes to security incidents, the business impact assessment, or analysis, evaluates the loss of confidentiality, integrity, and availability of organizational information systems.

In general, all coordinators during interviews emphasized that it is very "difficult to template", or "very hard to create processes" that unify steps regarding incident information disclosure. It is very difficult to learn from previous incidents, especially cyber ones, and use this knowledge to create effective disclosure strategies, since all the incidents always differ in details, in people that helped in mitigation, and in applicable regulations and timeframes.

5.3.2 *Harm mitigation and prevention*

1. *Global scale of the incident response operations;*

   Harm mitigation and prevention of security incidents builds around such activities as monitoring and reporting suspicious events, incident impact assessment, investigation and response, possible escalation of the incident to a different level, and incident closing and learning. There is a team in Malaysia that provides 24/7 operational support, incident classification, and incident recording to the database. After incidents are recorded, the company has around thirty incident managers globally trained to respond to them.

   The company operates in many different countries, and people who will be notified to handle the incident are determined by the level of the incident complexity and its location. Typically, incidents are handled locally, since people in the regions know better whom to talk to and who to involve. The incident owner would also be assigned from that region, perhaps with some supervision from the headquarters.

2. *Strong preferences towards the limitation of external notifications;*

   When an incident happens there is a triage process to evaluate its seriousness. If some vulnerability has been discovered, there is no necessity to report it externally; there are no regulations for it. But when it comes to vulnerability exploitation, the integrity of data cannot be guaranteed anymore. The company will have to choose between various options such as closing the breach and notifying stakeholders, or waiting and tracking what the threat agent wants to achieve, or even pursuing the hacker. The company will firstly focus on harm mitigation and prevention. Its main concern is that the attack is contained and all the business functions are restored to normal. To find the hacker is not a priority, the company will chase him only in case of a major incident.

   The company discloses incident information on a "need-to-know" basis. According to coordinators, a lot of people do not necessarily need to know about the incident. The company will share

incident information externally only if there is a necessity for external help (besides regulatory compliance issues). The company also does not inform everyone at the same moment, in order to avoid the information overflow. In every case there is always a trade-off - to act quicker and communicate information to other parties, or step aside and look at the incident from different angles for better comprehension of the situation.

With respect to voluntary sharing as the tool for harm mitigation, the company is the participant in several oil and gas networks, whom they might contact in case of a serious incident to see if others experience the same thing. Some information can be shared during semi-formal meetings of security specialists, but there are no formal processes that if "x" happens the company goes to the company "y". Typically, the company prefers to handle the incident on its own.

5.3.3 *Regulatory Compliance*

1. *Close attention to the regulations worldwide;*

   The company has legal experts as well as a global data privacy officer, who are contacted by the incident response team in order to clarify whether external notifications are required by law. Typically, the following types of data would fall under the scope of regulations:

   - Personal data;
   - PCI (also personal data but could be a company's credit cards);
   - Health data;
   - Export control data[3]
   - Terrorism attacks;
   - Intellectual property data.

   The company also discloses information to the U.S. Security and Exchange Commission, following their cybersecurity disclosure guidance, and already stated in one of the recent annual reports that the company experienced a serious APT attack that year.

2. *Strong preferences towards the limitation of external notifications;*

   Being aware that some laws require notification of certain incident within 48 hours, the company learned a special "trick" and

3 A particular case for U.S. (not requirement but advisable to do so) to avoid penalties. If data gets leaked to China or other embargoed countries, and it is U.S. export data, it is better to disclose the case. The penalties will be decreased if the company makes disclosure. When data is sent from the Netherlands to U.S., for example, it becomes U.S. data, so if it gets lost on the way back - it is an issue of U.S. export control data. Government can be involved since it is the violation of U.S. exports control.

do not call the situation "an incident", but, for example, "event of interest", before they know for sure what is going on, who is affected, and how to close the case. It will allow the company to extend the deadline for required external notifications. The company will just issue a short notice to governments or law enforcement that "something is going wrong, scope is not clear", and focus on incident mitigation.

If legal requirements to disclose are not applicable, the company will be interested not in what personal data the hacker has seen or stolen, but how he managed to get in, and how to protect the system from similar attacks. In general, it will prefer to stay quiet if regulations allow to do so and the public world does not know about the incident.

3. *Dependancy on the external legal networks;*

   Breach notification has to be done with the local law, and the company operates in many countries, as was mentioned earlier. To simplify the problem of complying with different regulations across the globe, the company has a rule to *"comply with that regulation that bites most."* If the disclosure strategy is compatible with the strictest regulation, it is compatible with all other regulations (e.g., for data export control the company uses U.S. level of export control, for other data types - EU level of notification duties). However, another problem immediately arises - that attacks are starting to have an international nature. Where the company should do disclosure is also becoming an issue. Is it in the land of discovery, in the land of damage, or in the land of the hacker?

   There is also a big confusion regarding the value chain. If some individual sends data to his bank account through the company's network, and it arrives to the bank in a different state due to, for instance, man-in-the-middle attack on https, then who is responsible? Was it the mistake of the bank, of the company, or just the lie from the individual?

   In all described confusing cases the company always asks for legal assistance. Legal people have connections to the government and court, and other legal experts around the globe, forming together a big network to find a solution for further actions. However, the company wants to move further than just relying on a legal network in their disclosure decisions. There is a need for policy that incorporates all notification duties and legal requirements for disclosure across all the locations the company operates in, so the company can reduce its requests to external legal advisors and thus increase its incident response capability.

5.3.4 *Cost-efficiency*

1. *Cost-efficiency has a lower priority among other disclosure preferences;*

   Cost-efficiency does take place in the company's decision-making regarding the most appropriate way of information disclosure; however, the company is big enough to cope with more expensive disclosure strategies if they will help in harm mitigation, compliance, or reputational issues.

2. *Strong preferences towards the limitation of external notifications;*

   There are specific cases when the company cares that their notifications are economically reasonable. For example, if there is an attack on operational infrastructures, the company will think twice before notifying the police, since it could require oil refineries to shut down for thorough investigation.

   Another example is that the company cares about its share value, therefore, in case of a serious attack, they will not share this information with their competitors, to prevent them from disclosing this information to the outside world and enticing the company's customers.

5.3.5 *Reputation*

1. *Reputation gains the priority in case of serious incidents;*

   Reputational exposure is indeed among the company's worries, but it is not that crucial if compared to financial or telecom institutions, where success directly depends on the trust and confidence of its stakeholders. Reputation becomes a big player only in the case of serious security incidents that can draw a wide response in case of the public announcements.

   As an example, several years ago the company were suffering from an APT and it took them two years to investigate what the attackers wanted to hack, how they came in, and whether they succeeded with their goals. The company was reluctant to communicate during the whole process; it wanted to understand all the details about the attack before making public statements. The only notifications made during that case were about help requests to the companies specialized in security.

   Media attention is quite controllable, according to the coordinators. The company has good security controls and procedures in place to be known widely as the company that does care about security. When it comes to situations with circulations of bad rumors or just incorrect information, it is not a problem for a company to release the notice that will change its external stakeholders' opinions.

5.3.6 *Business needs summary*

The majority of takeaways from the previous sections could be generalized, to a greater or lesser extent, in the business needs of an organization that is looking for better security solutions. Below, we summarized the major business needs when it comes to incident disclosure strategies:

— Internal notifications are based on the incident impact level discovered through the business impact assessment;

— A unified approach is employed to all kinds of security incidents;

— Disclosure takes into account the global scale of the incident response operations;

— Disclosure takes into account organizational preferences regarding the incident management;

— There is an opportunity to learn from the previous disclosure strategies;

— There is an up-to-date awareness of the regulations worldwide;

— Dependency on external legal networks is reduced;

These requirements should be implemented in the framework design to reach the intention of this research in solving an organizational problem. Later, it will be shown how each of the business needs is addressed in the proposed framework.

5.4 SUMMARY

This chapter presented a real company's approach on dealing with incident information disclosure, its main preferences and concerns. It was a good case study since it allowed us to get the feedback on the incident disclosure from the company that treats cybersecurity as a high priority, and takes into account all four introduced dimensions during the incident management process.

The collected information is related to the particular company and causes certain difficulties in attempts to generalize it. In the end of the chapter, we tried to summarize those business needs that might stay relatively the same across industries. We incorporate these needs in the final framework.

From the interviews we see that the major complexity of the current situation with respect to information disclosure - is the global scale of business operations. Whether it is about harm mitigation, or regulatory compliance, the company has to make decisions taking

into account geographic specifics of the incident. The core of the incident response will be conveyed at the location of the incident, not the location of discovery or main discussions, because external disclosures are shaped by the environment, and the knowledge of the environment, hence, becomes a valuable asset of the overall incident response.

The knowledge of all applicable regulations becomes another important asset, as we see from the interviews that the company wants to switch from reliance on external legal networks and accumulate the knowledge within the company.

Taking all these findings together, we see that there is a big need in having a system that uses as an input vector certain incident characteristics (e.g. location, scope of people affected, type of data involved), and creates an output with an appropriate incident disclosure strategy by mapping the received vector with corresponding notification requirements and recommendations from the knowledge databases. This idea will be discussed in the next chapter dedicated to the design of the incident information disclosure framework.

6

DECISION-SUPPORT FRAMEWORK ON CYBER INCIDENT INFORMATION DISCLOSURE

In Chapter 3, we determined the organizational challenges regarding incident information disclosure. In Chapter 4, we gathered recommendations from theory on how to deal with the identified decision problems, and in Chapter 5 we discovered the major business needs for the practitioners when it comes to incident notifications. The goal now is to synthesize advice from the literature with the business requirements, and to develop a framework that integrates all key findings and provides a generic guidance for arriving at an appropriate incident disclosure strategy. This framework will serve as an effective tool to guide decision making around cyber security incident notifications and help in defining the workflow of notification events.

Section 6.1 describes the main guiding principle behind the development of the decision-support framework, followed by its introduction in Section 6.2. The detailed discussion on how the framework incorporates the previous findings is given at Section 6.3.

6.1 THE FRAMEWORK PREREQUISITES

As mentioned earlier, every security incident has its specific traits. Accordingly, every organization has its own approach in doing business. With our framework we set several prerequisites to increase its overall utility and make it sufficiently generic to implement in a wide range of organizations. These prerequisites are:

— provide enough structure to enable the incident disclosure processes;

— give enough flexibility for organizations to customize the framework according to their operational settings;

— make the framework easily integrated into the existing business processes;

— incorporate strategic and tactical advice found in the literature;

— incorporate organizational business needs regarding incident disclosure discovered through the interviews;

— make the framework applicable for all kinds of security incidents, but also take the specifics of cyber incidents into account;

We do not consider the adjustment of the framework for specific needs in the scope of this research. Our goal is to design the generic decision-support framework, that will later allow the creation of concrete incident disclosure models tailored to the particular organizations.

6.2 THE DECISION-SUPPORT FRAMEWORK

6.2.1 *Design Approach*

In Chapter 1 we described the main idea behind the decision-support framework. Being a step-by-step guide, it should define a set of procedures which, when followed, will make it possible to access the problem environment as well as find the best solution regarding incident notification. The literature review and the disclosure approach of the interviewed company helped us to create a *generic timeline* of an average incident disclosure process. Below we summarize the major notification activities mentioned by the two sources:

— The timeline is tailored to the incident lifecycle consisting of six stages: *warning, risk assessment, initial response, management, resolution, recovery and learning*[1].

— The incident disclosure process starts once the security incident is confirmed and recorded in the system.

— Later, certain employees (e.g. from the service help-desk), after assessing the impact of the loss of confidentiality, integrity, and availability, inform the appropriate employees according to the pre-defined policy, who together compose an incident response team (IRT).

— After that, by analyzing more carefully the incident's details and organizational preferences regarding the incident mitigation, the team determines whether additional internal specialists have to be informed.

— The team also makes a decision on an external incident disclosure strategy, including people to be notified, content and method of notice, as well as more precise timeliness of notifications.

— Finally, in the recovery and learning stage, the team evaluates how the disclosure strategy has benefited or hurt the company, learns from this experience and optionally shares it with external parties.

The timeline (Figure 16) is a starting point in the framework design, as it allows us to map out the main activities and their order with

1 Six stages adapted from Chandler "Six Stages of a Crisis Model" [15].

respect to an evolving incident lifecycle. We want to mark out, to the extent possible, the common steps of the incident disclosure process and use them as a basis for the 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.

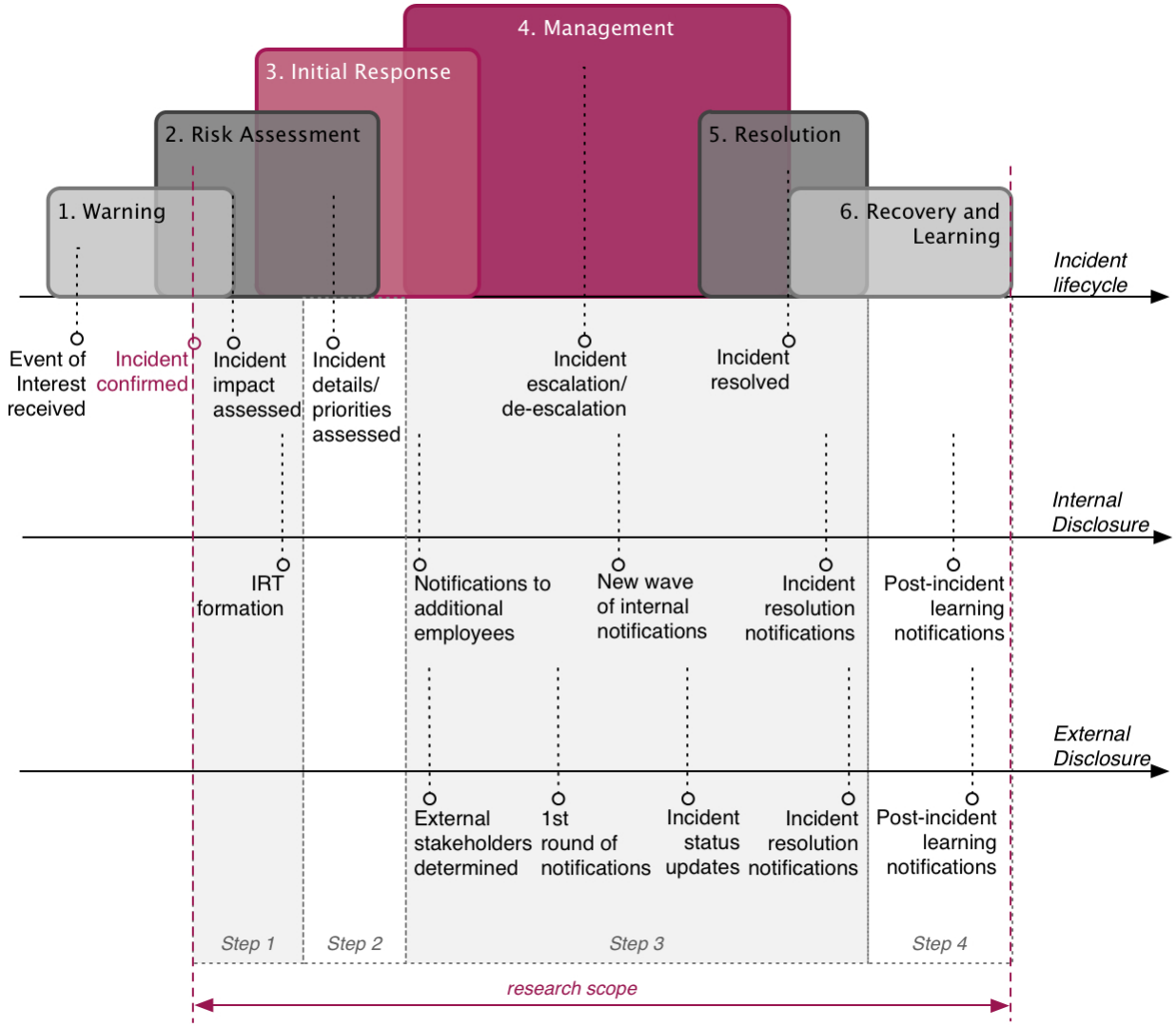


Figure 9: The Generic Incident Notification Timeline

We distinguished four common steps in the incident notification timeline that are relatively constant and will be followed with every security incident:

1. The incident impact assessment and the IRT formation in order to initiate the response process and harm mitigation;

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

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

4. Post-disclosure learning.

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

6.2.2 *Incident Disclosure Strategy Flowchart*

In this research we use a *flowchart diagram* to illustrate the framework approach. Our goal is to introduce a set of decision making activities to arrive on an optimal incident disclosure strategy, which correlates with the flowchart idea to present a step-by-step solution to a given problem. The flowchart shown at Figure 10 presents a generic algorithm on how to arrive on the appropriate incident disclosure strategy. It follows the four common steps introduced earlier:

Step 1. The process begins with the identification of the IRT composition through the *incident impact assessment*.

Step 2. Taking into account the specific nature of every incident as well as organizational preferences on how to solve it, details about the incident and organizational priorities should be clarified by filling in the *Incident Specifics Questionnaire* and *Incident Response Priorities*.

Step 3. This information together with incident status updates will serve as an input information for its further mapping with the content of the *Knowledge Database*. As the result, this mapping process leads to a decision on the most appropriate incident disclosure strategy with respect to the disclosure audience, timeliness, content and method of notifications.

Step 4. After notifications have been performed, the incident disclosure strategy is evaluated, filed and stored in the database for further reference.

The flowchart can be further extended to the cross-functional for the particular organization, where responsibilities for every process are assigned for certain organizational units. In this research, we do not specify who exactly within an organization performs the activities described in the flowchart; we assume though, that these people either belong to IRT from the beginning, or join the team upon request.

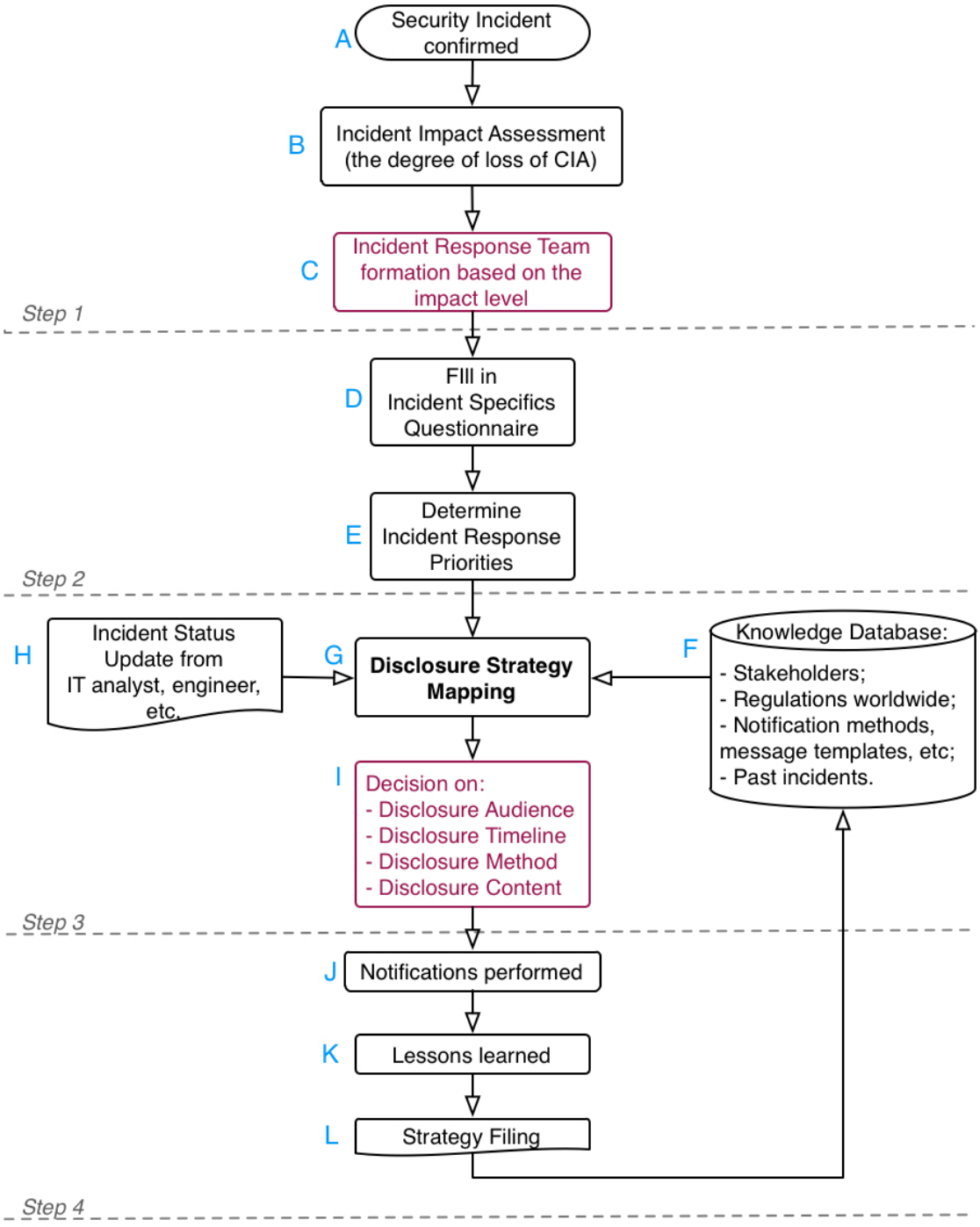


Figure 10: Incident Diclosure Strategy Flowchart

The next sections will 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 blue letter.

6.2.2.1 *First step. Incident Response Team formation*

As security incidents vary widely in their severity, the composition of the incident response teams 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 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).

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 scoring[2], that reflect the impact of loss of confidentiality, integrity, and availability of a company's information systems [62]. For the fast and correct IRT formation, a company may develop the 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.

Figure 11 gives an example of the incident level assessment process that is currently employed at the interviewed organization. Here, the incident impact assessment includes several categories, like financial, or operational loss to the company based on CIA aspects. The highest impact selected among these categories (which can be high, medium, or low) will eventually determine the incident level.

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. We would advise, though, following the recommendations from the literature and the interviews, to establish a position within a team for a person with the legal knowledge to make sure that all the decisions made during the IRT meetings have a legal base. In the case of advanced security incidents, the team should be cross-functional

2 An example of a potential impact scoring can be found in Appendix F.

and involve (at least) coordinators from the incident response management team, the privacy office, corporate communications, senior management, and the legal department.

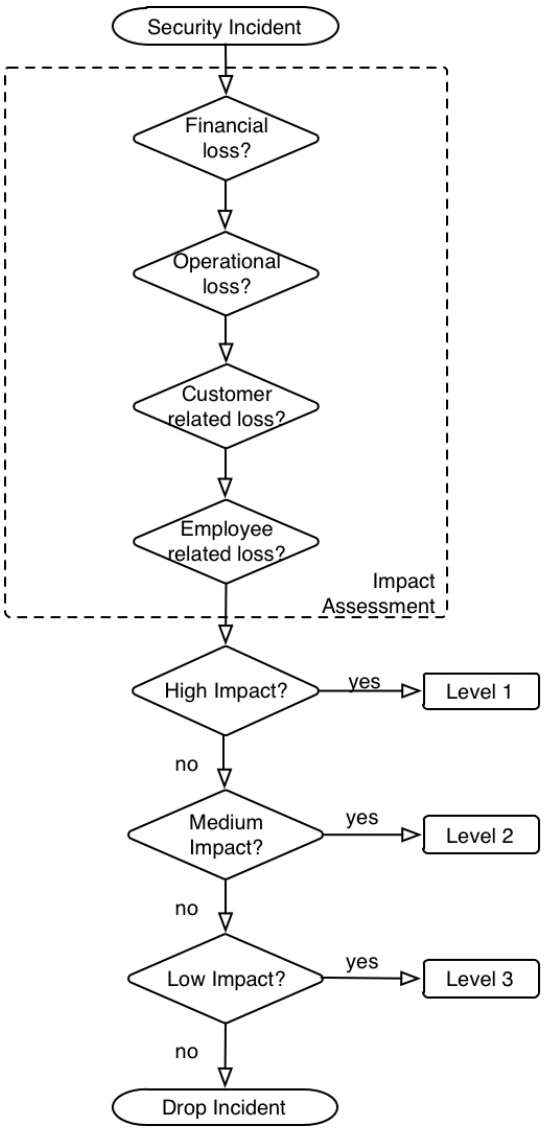


Figure 11: Incident Level Assessment Process. Adapted from the Interviews, Chapter 5

6.2.2.2 *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 we need to have a process in place that will help to summarize all key incident details that affect the disclosure decision.

In this research, after thorough examination of organizational challenges and dilemmas, as well as all sorts of recommendations, we developed a list of questions to assist in describing the incident specifics, which would influence the disclosure strategy of the company. We call this list *"Incident Specifics Questionnaire"*.

Figure 12 shows an example of a possible questionnaire, where we included the questions that 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. For example, if a company is not listed at NYSE, it does not need to consider the question of the incident materiality and notification to U.S. SEC. At the right side of the questionnaire we give an example on how the answers will help later to determine the disclosure audience, such as internal specialists and external third parties.

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 existing knowledge base on incident information disclosure. For instance, if personal data was stolen, and it was not encrypted, a company will have to immediately notify affected individuals if regulations in the incident location(s) require doing so.

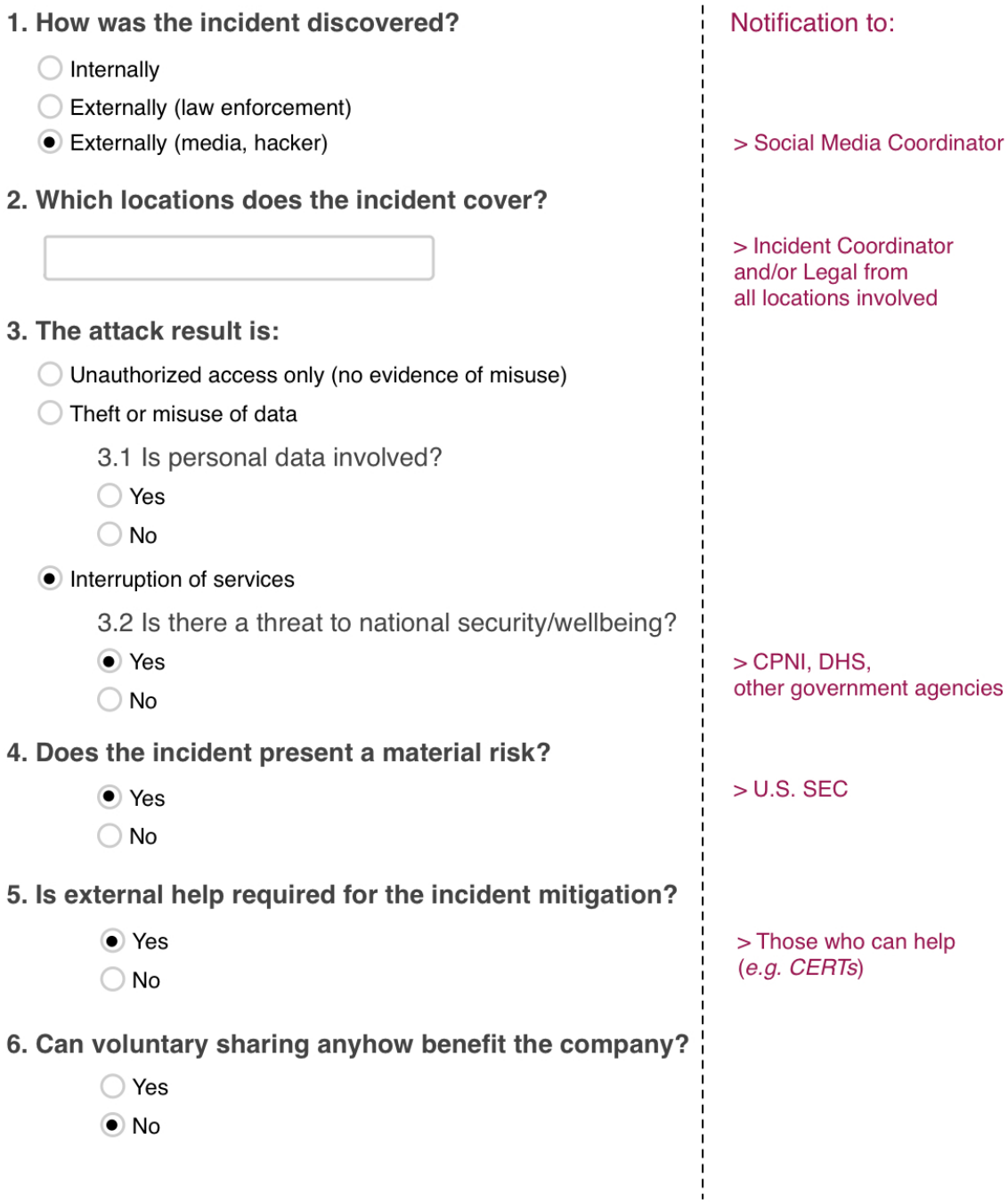


Figure 12: Incident Specifics Questionnaire Example

E: Incident Response Priorities.

What we discovered in the previous chapters is that any organization always has some preferences that determine its willingness to disclose the incident information. We presented four dimensions that form these preferences: harm mitigation, regulatory compliance, cost-efficiency, and reputation. The disclosure strategy should not be based solely on what regulations require; 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 the 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 [42]. They suggest using a tool called *incident response priority sliders* (Figure 13) 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. In the beginning, all the sliders are at the middle, and every step towards maximum for one objective will require one step backwards for another.

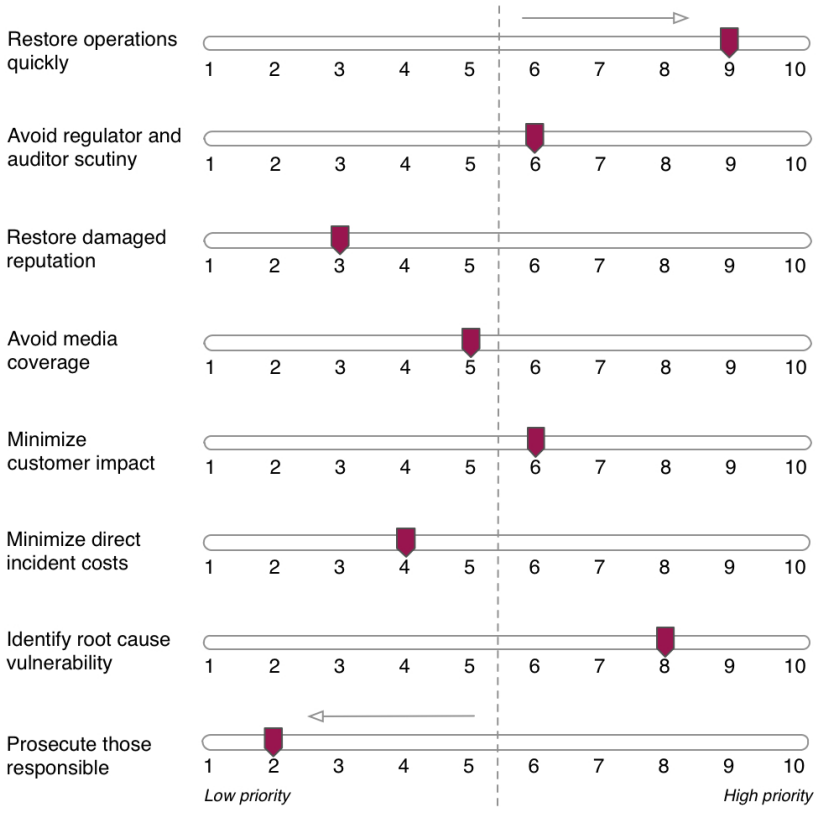


Figure 13: Incident Response Priority Sliders. Adapted from [42]

We believe that incident response priority sliders also clearly determine a company's priorities regarding the incident disclosure. The list of alternatives at the left side is formed by the influence of the four dimensions. For example, a company that put sliders in a way as shown at the Figure 13, will first focus on the restoration of all affected operations and the identification of the incident cause. Only after that will they think about giving notice to regulatory authorities or affected individuals, as reputation or financial concerns are not among its priorities. This 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 what happened is absolutely correct.

Incident response priority sliders will help to clearly mark out what an organization wants to achieve with its disclosure strategy. Together with the incident details they will compose a complete set of prerequisites that will influence the choice of the 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.

6.2.2.3 *Third step. Disclosure Strategy Mapping*

After the incident details and a company's priorities have been identified, the IRT can start the actual process of arriving on 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), which stores the up-to-date lists of regulations, stakeholders' contacts, notification scenarios and message templates, etc. We call this process as *Disclosure Strategy Mapping* (H), since the outcome 1of this 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 cri-

sis 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 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. While the overall approach may vary among organizations, the database architecture should meet certain requirements to be an effective framework tool. We define the requirements as follows:

1. restricted access for authorized personnel (e.g. the incident response team members only);
2. access through a website/application which is protected by username and password;
3. 24x7 accessibility, also through VPN connection;
4. large storage capacity (to store best practices, regulations, policies in .pdf, .doc, .xls formats);
5. upload/modify functionality according to the privileges of database users;
6. functionality to run queries on the stored data (to enable the questionnaire and tags/keywords search);
7. periodical review (to make sure that information is up-to-date);

G: Disclosure strategy mapping.

Disclosure strategy mapping is the main process in our decision support framework. 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 every possible security incident scenario to determine which information is required for the database. In this research, we present the minimum required information, such as applicable legal requirements, a company's stakeholders with up-to-date contact information, and some incident disclosure templates.

H: The Incident Status Updates.

An important scenario to consider is 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 BIA and incident questionnaire stages. 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.

6.2.2.4 *Fourth step. Post-disclosure learning*

Our framework allows a company to start learning from the disclosure activities. Even though we discovered from the interviews that security practitioners tend to think that it is hardly possible to learn from the previous security incidents, we argue that 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 at, for example, the Netherlands, as it was at 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 our 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 (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).

6.3 THE FRAMEWORK AS AN INTEGRATIVE TOOL OF PREVIOUS FINDINGS

As we mentioned in Section 6.1, one of our main prerequisites is to incorporate strategic and tactical advice found in the literature, and also to address organizational business needs regarding incident disclosure discovered through the interviews. Table 4 shows where in the framework we implemented the collected recommendations and organizational requirements.

6.4 SUMMARY

This chapter presented a decision-support framework for security incident information disclosure. It comprises a generic incident disclosure flowchart that built upon the four processes that we discovered to remain relatively constant with every security incident. These processes are: 1) incident level assessment and formation of the IRT with respect to level; 2) further assessment of the incident specific details as well as organizational priorities regarding the incident response; 3) the incident disclosure strategy development and realization; and 4) post-disclosure learning.

The major advantage of the developed framework is that it clearly defines all the steps in the deciding on a security incident disclosure strategy. Currently, no frameworks like that exist, there are only scattered recommendations across the scientific and business literature. We analyzed and integrated these recommendations in the flowchart: it incorporates the major strategic advice, as such as it enables the fast IRT formation, or considers incident response priorities of the organization which makes the final disclosure strategy not only compliance based. The framework also gives some leeway to employ the tactical advice by adding it to the knowledge repository and referencing this information when needed.

The framework responds to the practitioner requirements to consider different kinds of security incidents, and it can still address cyber incidents by either adding specific questions to the questionnaire, or creating the cyber specific sliders, or storing the cyber related information in the database. The flowchart processes themselves are not technically complicated to employ it within any company, and they are flexible enough to be readjusted for the particular needs.

The next step is to evaluate the framework by using several incident scenarios and also asking for the opinion of a security specialist, to see whether the flowchart process indeed reflects current business needs, the pitfalls it possesses at the current stage, and what can be improved upon.

	What to integrate:	Where in the framework:
Strategic advice	— The incident response team is informed prior to any other notifications. Its composition reflects the impact level of the incident.	Incident impact assessment, IRT formation;
	— Different notification triggers to certain stakeholders depending on the incident result (e.g. unauthorized access, theft or misuse of data, or systems disruptions); — Regulations check once the incident is confirmed, on the required notification audience;	Incident Specifics Questionnaire, Knowledge Database
	— Voluntary sharing as a possible harm-mitigation or reputation restoring tool; — Notifications timeline adjustment depending on the legal requirements, incident details, and organizational priorities in the incident response; — Content and amount of information to release reflects the incident details; — Communication channels should be chosen in accordance with the incident details;	Incident Specifics Questionnaire, Incident Response Priorities, Knowledge Database
Tactical advice	— A pre-defined list of employees with their contact information that are involved in the incident depending on its impact level; — A pre-defined list of employees with their contact information that will further join the incident response team based on the incident specific details; — Create and update the contacts of external counsel as well as companies specializing in crisis communications and incident response that might help once there are not enough internal resources; — Create and update the contact information of third parties that might be involved in the incident and should be notified prior to any public announcements, to be prepared for future inquiries; — Create and maintain the message mapping database with different notification templates related to different stakeholder groups, types of security incident, or incident stage; — Create and maintain the list of the preferred notification methods depending on the location specifics, affected stakeholders, and regulation requirements (postal mail, emails, phone calls, etc);	Knowledge Database
	— Try to avoid early public notifications, before all the information is available about the incident. If delays are not possible, incident status update should be established to quickly re-adjust the disclosure strategy;	Incident Status Update
Business needs	— Internal notifications are based on the incident impact level discovered through the business impact assessment;	Incident impact assessment, IRT formation;
	— Unified approach is employed to all kinds of security incidents;	The entire framework
	— Disclosure takes into account organizational preferences regarding the incident management;	Incident Response Priorities
	— Disclosure takes into account the global scale of the incident response operations;	Incident Specifics Questionnaire
	— Ability to learn from the previous disclosure strategies; — Up-to-date awareness of the regulations worldwide;	Incident Specifics Questionnaire, Knowledge Database
	—Reduced dependency on external legal networks.	Notifications performed, lessons learned, strategy filing

Table 4: Integration of the previous findings in the framework

7 FRAMEWORK EVALUATION

The final phase of this research is dedicated to evaluation of the designed framework. Our goal is to connect dots and show that the framework indeed deals with the identified set of decision-making challenges from Table 1. Additionally, we examine the quality of the final framework via evaluation methods such as showcase scenarios (Section 7.2) and an interview with a security expert (Section 7.3). The expert interview also serves as the first step in the process of communication of the research findings.

7.1 FRAMEWORK EVALUATION USING IDENTIFIED CHALLENGES

During the analysis of the problem environment in Chapter 3, we determined a set of challenges a company has to deal with while developing an incident disclosure strategy. The final goal of the framework is to help organizations address every challenge from the list, so they can find an appropriate solution that will be in line with organizational needs and external requirements.

Hence, the first test of our framework would be to show that it does address all identified challenges from the four categories "To whom", "When", "What", and "How". In Table 5, we list all the challenges together with explanations how the framework will help in solving the issue.

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. 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 column *"Framework solution"* shows what framework tools are being used in order to obtain information required to resolve each challenge.

Category	Challenge	Framework Solution
	Harm mitigation and prevention	
"To Whom"	Identifying the right stakeholders to be informed for effective incident response and harm mitigation	Inicdent 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

Table 5: Framework Solution for the Identified Challenges

7.2 FRAMEWORK EVALUATION USING SECURITY INCIDENT SCENARIOS

In the previous section we presented the framework solutions for the identified challenges. In order to show their feasibility, and also explain in more details how the flowchart processes work, we developed two security incident scenarios[1]. The blue letters indicate which process of the flowchart (Figure 10) is being described.

7.2.1 *Scenario 1: U.S. server goes down*

Incident details:

- U.S. server has been compromised;
- no access, the password has been changed;
- no information on what kind of data is stored on the server;

STEP 1.

B: As soon as this incident is confirmed, the Service Desk assigns the impact level to it based on the predefined impact assessment policy. This policy specifies definitions of high, medium, and low levels of impact with respect to confidentiality, integrity, and availability. The incident details are compared with the definitions, which allows to determine the total impact. For example, in the current situation, when there is no evidence that sensitive data was stored on the server (low impact on confidentiality), but it has been unavailable for quite a long time (medium impact for integrity and availability), the company may arrive on the following impact scoring:

Impact Level={(confidentiality, LOW), (integrity, MEDIUM), (availability, MEDIUM)}= MEDIUM = Level 2

C: The company has a predefined list of employees with their contact details who will be informed in case of a Level 2 incident. They will constitute the initial incident response team. For Level 2 incident, it can be IT services, Operations Manager, CISO, Deputy CIO.

STEP 2.

D: Now the team continues the investigation. As part of the incident response it should define wether additional employees have to be notified, and whether external notifications are required. The team

1 Several ideas for the scenarios were adopted from the NIST security guide [64]. We also consulted with the security specialists from ISC division, KPMG, to ensure the feasibility of the designed cyber incidents.

member fills in the questionnaire (Figure 12) with information available at the moment, and retrieves the following documents from the database:

1) How was the incident discovered?
IF "Internally" ⟶ "Communication_procedure_int.pdf"

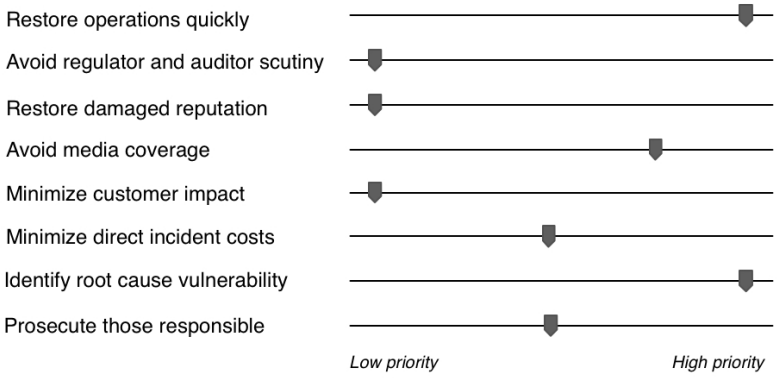
2) Incident location?
IF "USA" ⟶"Disclosure_policy_US.pdf"

3) The attack results in?
IF "Unauthorized access" ⟶ "Un_access_contacts.csv"

4) Does the incident present a material risk?
IF "No" ⟶ NA

5) Is external help required for the incident mitigation?
IF "No" ⟶ NA
...

E: At this moment, it is unlikely to have a big dispute around organizational disclosure priorities (Figure 13). While the incident remains an internal issue, the company will assign the high priority to *"restore operations quickly"* and *"identify root cause vulnerability"*, and it will also try to let the incident stay within the company by focusing on *"avoid media coverage"*, as shown below:



STEP 3.
F-G: The following documents will be retrieved from the database as part of the requested information in the step 2:
Communication_procedure_int.pdf will provide the general approach to internal notifications within the company, *Disclosure_policy_US.pdf* will show that external disclosure is not obligatory in the U.S. if there was unauthorized access only, and *Un_access_contacts.csv* will gener-

ate the contact list of employees who can assist in dealing with the incident that resulted in unauthorized access.

H: Meanwhile, the IT analysts determine that there was client data stored on the server including names, contact details, and SSN, and that the attacker stole some of this data which was not encrypted. The incident status update is sent to the IRT. It is a crucial change for the designing a disclosure strategy, so the team quickly requests the new information from the database.

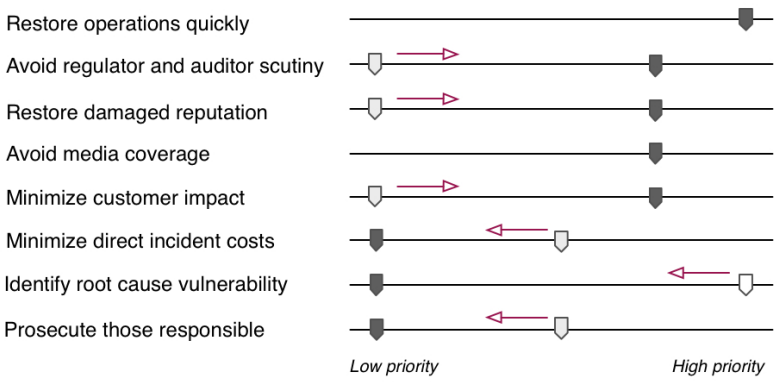
1) The attack results in?
IF "Theft/misuse of data" $\longrightarrow$ NEXT QUESTION

2) Is personal data involved?
IF "Yes" $\longrightarrow$ "Privacy_policy.pdf" AND "Privacy_contacts.csv"

F-G: *Privacy_contacts.csv* will generate the contact list of employees required to be notified in case of personal data breach incidents. It can include, e.g. Privacy Coordinator, HR and Legal officer.
Privacy_policy.pdf will provide the organizational policy on how to deal with privacy data issues, also with respect to information disclosure. The previously retrieved *Disclosure_policy_US.pdf* will used as the source of data breach notification duties.

After the incident update, the priorities would also change. The Deputy CIO may still insist to *"restore operations quickly"*, but now the incident falls under scope of the U.S. regulations, and requires external notification. So a legal advisor can insist on increasing priority of *"avoiding regulator and auditor scrutiny"*, *"minimizing customer impact"* and be prepared to "restore damaged reputation". It will force to lower the priority of certain objectives, as shown below.

By adjusting sliders, the team can agree on the approximate timeline of notifications, and also involve additional parties to help in achieving the highest priorities. In this case it can be Social Media Coordinator, or third parties specialized in crisis communications.



STEP 4.

J-L: After the incident is solved, a team member creates a report describing the steps made regarding internal and external disclosure (possibly with evaluation comments), assign keywords or tags, and store it in the Knowledge Database. For this particular case, such tags as *"personal data"*, *"u.s."*, *"web server"* can be used. In future similar cases, when filling in the questionnaire, the team will be able to retrieve the report by searching through the existing tags.

7.2.2 *Scenario 2: Attack on the industrial control systems of the chemical plant*

Incident details:

- the plant is located in the U.K.;
- unauthorized commands issued to the control equipment;
- very soon, the operator screens go blank and the system is shut down;
- potential risk of environmental incident;

STEP 1.

B: The IT analysts at the power plant determines that the SCADA system processes only sensor data, so the potential impact from a loss of confidentiality is LOW, however there is a high impact from a loss of integrity (there were unauthorized commands) and availability (the access to the system is completely disrupted). Hence, the total impact level is:

> *Impact Level*= {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)} = HIGH = Level 1

C: The company has a predefined list of employees with their contact details who will be informed in case of a Level 1 incident. They will constitute the initial incident response team. For Level 1 incident, it can be IT services, Operations Manager, Business information risk manager, Legal, HR, CISO, CIO.

STEP 2.

D: Now the team continues the investigation. As part of the incident response it should define wether additional employees have to be notified, and whether external notifications are required. The team member fills in questionnaire (Figure 12) with information available at the moment, and retrieves the following documents from the database:

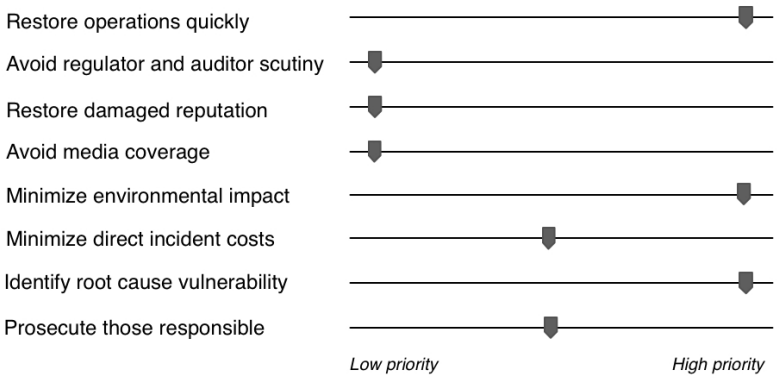
1) How was the incident discovered?
IF "Internally" ⟶ "Communication_procedure_int.pdf"

2) Incident location?
IF "UK" ⟶"Disclosure_policy_UK.pdf"

3) The attack results in?
IF "Interruption of services" ⟶ "Interruption_policy.pdf" AND "Interruption_contacts.csv"

4) Is there a threat to national security/wellbeing?
IF "Yes" ⟶ "governmental_contacts.csv"
...

E: As of now, the incident is mainly an internal issue that also requires the assistance of certain governmental agencies since there is the risk of environmental damage. In such situations, the team will assign the highest priority to *"restore operations quickly"* to ensure authorities that the situation is back to normal, and *"identify root cause vulnerability"*, to guarantee that the incident will not happen again. The company will also focus on *"minimizing environmental impact"* to ensure that no damage is caused to the environment.



STEP 3.
F-G: The following documents will be retrieved from the database as part of the requested information in the step 2.
Communication_procedure_int.pdf will provide the general approach to internal notifications within the company,
Disclosure_policy_UK.pdf will provide regulations related to Industrial Control Systems (IDS), and *Interruption_contacts.csv* will generate the contact list of employees who can assist in dealing with the current incident. *Interruption_policy.pdf* or other similar documents should exist in any industrial company that describes incident mitigation steps in case of systems interruptions, also related to information disclosure.

By adjusting sliders, the team can agree on the approximate timeline of notifications, and also involve additional parties to help in achieving the highest priorities. In this case it can be CPNI (Centre for the Protection of Critical Infrastructures) and environmental agencies.

STEP 4.
J-L: After the incident is solved, a team member creates a report describing the steps made regarding internal and external disclosure (possibly with evaluation comments), assign keywords or tags, and store it in the Knowledge database. For this particular case, such tags as *"chemical plant"*, *"UK"*, *"availability"*, *"interruption"* can be used. In future similar cases, when filling in the questionnaire, the team will be able to retrieve the report by searching through the existing tags.

7.2.3 *Scenarios overview*

The discussed incident scenarios make it more clear how the framework automates the decision-making around incident disclosure issues. The framework utility and efficacy heavily rely on the content of the knowledge database, as we see from examples. The database can store ".csv" files with contact information, ".pdf" or ".doc" files with policies, regulations worldwide, or best practices around disclosure.

Overall, once a company adjusts the incident disclosure framework to its needs, it should consider using past security crises to test its own disclosure approach. It is required to guarantee that the framework will work during a real incident. There are a lot of examples of cyber attacks that happened to big corporations, like Sony, RSA, KPN in recent years, that can be used as a template to test what would be the organizational notification steps in those cases, and compare its approach with reality.

7.3 FRAMEWORK EVALUATION THROUGH EXPERT INTERVIEW

As the framework design was partly based on the information received from a single company in a specific industry, it would be beneficial to validate the final approach with a different organization. It should satisfy the same requirements as we set up for the interviews from Chapter 5. The company should look beyond technical solutions in response to cyber incidents and be interested in the implementation of security policies and procedures that will facilitate an effective incident response. Additionally, there should be a high probability that harm mitigation, regulatory compliance, cost-efficiency, and reputation are among organizational preferences when developing incident disclosure strategies.

We found a chance to introduce the framework to the Head of Information Risk Management of a large financial company[2] during a one-hour interview. The financial sector is highly exposed to a diverse range of cyber attacks, hence the company has a profound experience in dealing with security incidents. This gave us a good opportunity to compare the framework with the current state-of-the-art regarding incident disclosure within a company, find which ideas behind the framework are valuable, and what may require improvement.

After the short framework introduction in the beginning of the interview, further discussion was held around the two following questions:

1. Would it be possible to implement such framework within the company?
2. Would it add value?

Bellow, we summarize the major comments regarding these questions with a short evaluation overview in the end.

7.3.1 *The framework implementation possibility*

According to the interviewee, in order to implement the framework within a company, we should base it on the current incident management procedures that are relatively similar across organizations. Large companies already have policies in place to handle security incidents, which can be improved by building in certain steps that will simplify the incident disclosure process.

Our framework, in general, correlates with the current company's approach to perform incident disclosure. The company implements the incident impact assessment to mark security incidents out of many others. It also performs further incident assessment in order to pass the security incident to the appropriate employees (some security incidents will require special assistance of internal employees, like a press or HR officer). The company assesses the impact based on different criteria: the scope of the incident, how many services were interrupted, how many people affected, is there any information in the media already. This corresponds with our first step in the flowchart about incident impact assessment and the IRT formation, and later assessment of the incident details via the questionnaire.

Currently, such framework tools as the questionnaire or priority sliders do not exist within the company, and thus will require time and effort to implement. These details are clarified during the meeting discussions of the incident response team. A special concern goes to the knowledge database, where the interviewee expressed some doubts about the overall possibility of collecting large amounts of information required to support the disclosure decision. A company

2 For security reasons, the company's name cannot be disclosed in this research.

may operate in many locations or experience a big variety of security incidents, so identification and collection of local regulations, best practices around notifications, etc, could become a very difficult task. Proper selection, "filtering", of the possible security incidents would be essential to simplify the process of finding the relevant information for the database.

7.3.2 *The framework added value*

The interviewee sees the main value of the framework in its mapping process that allows to extract the best practices on incident information disclosure from the database. To be able to do so, it would be necessary to make a big preliminary work on preparing the best practices depending on the location, applicable disclosure regulations, type of the incident. But once such information is available, it would enable the fast overview of the steps required to inform internal and external audiences. At the moment, there are no procedures or best practices stored that will assist in defining whom to contact in a particular country after a particular incident.

If the company has a good organization of its local branches with employees knowing well local regulations, media channels, etc, there will be less need in automation of the decision making process regarding incident disclosure. The value of the framework increases with more complicated global scale of operations, where a lot of decisions should be approved by headquarters, or there is a poor knowledge of existing and upcoming regulations in the industry worldwide.

Regulations and high media coverage of security incidents typically require quick reaction from organizations in their incident information disclosure. With our framework we wanted to automate the process of developing the incident disclosure strategy, so it can be done faster without affecting the quality of decisions. During the interview we discovered that delays in disclosure, even if it leads to a penalty, is not a big issue for the particular company. Its main focus is to ensure complete recovery and business continuity. Therefore, in case of an incident, it will shortly inform the regulator that something is going on, and then take one or two weeks to investigate before any other external disclosures.

Additionally, as the company always put the highest priority on the restoration of its operations, the option *"restore operations quickly"* at the priority sliders would be excessive, at least for this particular organization.

7.3.3 *Feedback Overview*

Based on the received feedback we can compare the proposed framework steps with the current approach to disclosure within the company:

— Step 1 on incident impact assessment and the IRT formation is already in place within the company;

— Step 2 on clarifying the incident details and organizational priorities is not automated, as suggested by our framework, but exists as part of the incident response team discussions;

— Step 3 on disclosure strategy mapping is not present. There is no knowledge database that could support the disclosure decision. However, it was acknowledged that such database would add the value to the current process of arriving on the incident disclosure strategy;

— Step 4 on post-incident learning from the disclosure strategies is not present. Still, we consider it as a valuable process since it provides the addition to the knowledge database (the disclosure report file), and thus increases its overall utility.

We think this comparison proves that we set the right direction for the framework approach; nonetheless, there is always a room for improvement. Below, we summarized some major comments from the security practitioner that would be useful to consider in future work:

— the knowledge database is the major source of value for the framework; a lot of attention should be paid to its structure and content;

— storing best practices on incident disclosure influenced by regulations and types of security incidents would increase the overall value of the framework;

— some organizational priorities, e.g. services recovery, will remain constant regardless of the incident, and thus will influence from the beginning decision-making around disclosure.

In general, during the discussion we observed that different industries might place incident disclosure at different problem levels. There could be various explanations for it, but we think that the main reason lays in the scope and complexity of organizational business operations, and thus in the increasing amount of information required to make right disclosure decisions. For example, industries that are strictly regulated in terms of disclosure (such as financial or telecom providers, by operating with large amounts of personal data), are

better prepared for notifications when a real incident occurs. As a matter of survival, they are fully aware of the required legal steps and perform disclosure on a regular basis. In contrast, the oil and gas industry is a more complex environment that includes but is not limited to operations with personal data. As a consequences, external requirements are growing as well as different depending parties, which makes it more difficult to make timely and relevant incident disclosure decisions.

7.4 SUMMARY

In this chapter we performed the final phase of this research - the framework evaluation. We tested the utility and efficacy of the proposed framework by applying it to the identified challenges; by running two security incident scenarios; and by discussing the approach with the security expert of the large financial company.

We discussed how the framework tools are being used in order to obtain information required to resolve each challenge regarding the audience, time, methods and the content of security incident notifications. This information serves as a key deliverable for incident response meetings in order to arrive at the efficient disclosure strategy under time pressure.

Incident scenarios helped clarify the framework workflow, and show how the introduced tools such as priorities or retrieving data from the database can be actually performed. We showed how the database can help make decisions regarding the disclosure faster, if there is a sufficient amount of information stored in it. Hence, the creation of the database is becoming a crucial issue in order to make the whole framework worth implementing.

The expert interview helped us understand what difficulties can be associated with the implementation of the framework in the company. We also received some feedback on its overall value. The major change the framework makes to the business world is that it automates the process of decision-making regarding incident disclosure, while 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.

8 CONCLUSIONS AND CONTRIBUTIONS

In this research, we present the decision-support framework on organizational disclosure of cyber security incident information to internal and external stakeholders, which facilitates incident response in line with organizational goals and existing requirements.

In order to design the framework, different research phases have been accomplished, including investigating a wide range of scientific and industry papers, asking security practitioners about their needs regarding incident disclosure, integrating the received information in the framework, and undertaking an evaluation process of the designed flowchart.

In this chapter, we summarize the main contributions of the present work, discuss research limitations, and suggest potential ideas for future work.

8.1 MAIN CONTRIBUTIONS

We identify the following contributions of this research:

1. The research dives into cybersecurity challenges of modern corporations and finds evidence of the importance of incident information disclosure in organizational crisis management activities.

2. The research identifies four key dimensions of organizational security incident information disclosure (Figure 7). These dimensions create a set of challenges for a company to deal with regarding notification audience, time, content, and methods, which are explicitly listed in the report (Table 1).

3. The scattered advice from numerous scientific and industry papers is combined into two clear sets of strategic and tactical advice (Table 3);

4. The proposed decision-support framework (Figure 10) integrates key findings and addresses every identified challenge, assuring rigor and relevance of this study. The introduced framework tools, such as Incident Specifics Questionnaire (Figure 12) and Incident Response Priorities (Figure 13), 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. Intended as a solution for cyber security incidents only, the framework can eventually be applied to all types of security incidents, which increases its overall value.

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, with our framework we came a step closer to a more intelligent approach to cyber security incident response, by allowing companies to decide faster 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.

8.2 RESEARCH LIMITATIONS

This research is not without some limitations. The major one is that we used only one company as the source of business needs regarding incident disclosure, and based some elements within the framework on this industry-specific information. Different industries have different types of relationships established with their key stakeholders; besides, regulations vary a lot depending on the industry sector. Therefore, what can be a disclosure problem for one company, would be just a minor issue for another. Initially, it was planned to interview five different industries (energy, financial, telecommunications, governmental, educational) to gain more profound overview of the current problems related to security incident disclosure. Unfortunately, it did not work out as intended, when certain companies did not manage to find time for interviews.

Another limitation (and hence opportunity for further research) is the lack of empirical testing of the framework in a realistic environment. It requires large commitment in time and resources from external organizations, which in the time frame of this research was not feasible to organize. As of now, feedback was received from only one security expert, so there is a risk of getting an unrepresentative view of concrete industry. The positive moment though, is that we see some interest in the disclosure procedures from other companies, so there are opportunities to continue testing the framework in the near future.

Finally, in this research we do not discuss in detail how the framework tools, such as incident impact assessment or knowledge database, should be implemented to ensure the overall effectiveness of the frame-

work. We assume that these elements will be implemented in a company, but we do not provide explicit solutions for their installation, assuming that different companies may do it in different ways. However, as we discovered by the end of the research, being more detailed could help to increase the overall value of the framework and also find the framework pitfalls. Hence, we recommend to provide the framework tools in a greater detail in the future work.

8.3 FUTURE RESEARCH POSSIBILITIES

This research is a first attempt in the process of automation of decision-making around security incident disclosure. There is still a lot to investigate, discover, implement.

The limitations mentioned in the previous section serve as the base to continue investigating security incident disclosure issues. More companies could be asked for feedback to discover whether some industries value the framework solution more than others, and if so, which ones. Future adjustments to the framework should be based on the comments of those organizations that see value in implementing a more automated process of arriving on an incident disclosure strategy.

As this report progressed, we noticed that there is a benefit in exploring the technical implementation of the tools proposed by the framework. Companies would like to see that it is feasible to create the proposed database with a big amount of different information; that it would be easy to retrieve the data which will help in making judgment calls regarding security incident disclosure. Hence, by designing the generic applications proposed in this paper (e.g. incident specifics questionnaire, knowledge database), future researchers will help promote the decision-support framework among the companies. Applications will also assist in testing the framework's utility and efficacy and proposing future changes.

Finally, the scope of this research does not consider activities prior to the confirmation of a security incident. However, the process of moving from an event of interest stage to the actual confirmation of the security incident could require a lot of time and possibly extensive internal disclosures. As we discovered from the interviews, the company can continue naming the actual incident as an event of interest, just to take delays before external disclosures, since regulations require disclosing the incidents that have been confirmed. It would be interesting to see how the incident labeling can influence the disclosure decisions, and how organizations can potentially benefit from it.

A

DESIGN SCIENCE RESEARCH METHOD

A.1 INTRODCUTION TO DESIGN SCIENCE

Hevner et al. describe *Design Science* as a paradigm in which the creation of a useful *artifact* is set as the main goal rather than developing or verifying theories. Design science effectively addresses so-called *wicked problems* [66] that exist in unstable environments, where complex interactions between sub-components exist, or there is a critical dependence on human cognitive and social abilities to produce effective solutions. An environment of this research - the rapidly changing level of cyber threats, new regulations, organizational dependency on human decision-making skills in addition to IT systems, and complex interconnections between people managing security incidents - creates, thus, a set of wicked problems need to be solved in order to produce a useful artifact.

A step-by-step decision-support framework, an outcome of this research, can be classified in the design science vocabulary as a *method*. According to Hevner et al. methods "define processes. They provide guidance on how to solve problems, that is, how to search the solution space. These can range from formal, mathematical algorithms that explicitly define the search process to informal, textual descriptions of best practice approaches, or some combination" [19]. In the context of this research, a framework will define a set of procedures following which it is possible to access the problem environment and find the best solutions on how, what, when, and to whom disclose cyber security incident information.

A.2 DESIGN SCIENCE RESEARCH FRAMEWORK

A specific design science framework selected for this research was firstly proposed by Hevner et al. and later refined by Wieringa. It is a model that is widely used and referenced a lot in the related publications, which suggests the high quality of the selected framework. The model also presents a set of guidelines to follow for delivering a good design science project, which will be discussed in the next section.

According to the framework, a design science project is a set of nested problems in which the top level problem is always a *practical* problem. The main question of this research is a practical problem on designing an organizational framework, which is decomposed into set of knowledge subproblems (Q1-Q4) and practical subproblems (Q5).

Figure 14 presents the design science framework for understanding, executing, and evaluating this research. The *environment*, which is composed of people, business organizations, their technologies, and existing regulations, determines the problem space. Elements within this environment define the current *business needs*, and research activities should address these business needs to assure research relevance. The *knowledge base* provides the practice - oriented theories to assure rigor of the study. The design science research space contains a number of practical and knowledge problems to deal with, as described earlier. *Knowledge problems* are solved by applying knowledge from the knowledge base or by using data obtained through the interviews. *Practical problems* are solved by matching problems and solutions after analysis of information gained from the answers on knowledge questions as well as understanding of the problem environment.

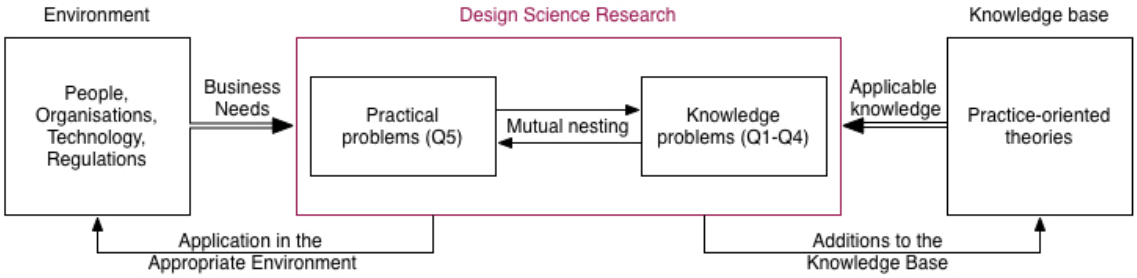


Figure 14: Design Science Research Framework

A.3 DESIGN SCIENCE RESEARCH GUIDELINES

An effective design science research, according to Hevner et al., should follow seven guidelines. Table 7 presents these guidelines and describes how this research is intended to meet them in order to guarantee the quality of the final work.

Guideline	Hevner Description	In this research
Design as an Artifact	Design science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.	The decision-support framework on security incident information disclosure satisfies the criteria of an artifact. As described earlier it is a *method* that provides guidance on how to solve the practical problem.
Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	The research problem has been formed after the preliminary analysis of current organizational problems in the cybersecurity field. An interest in the framework from the interviewed practitioners also proved importance and relevance of the study.
Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	Incident scenarios and an expert opinion are being used to evaluate the framework.
Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.	The research project seeks to fill the gap in the existing knowledge (design foundations) on cybersecurity incident notification by introducing a novel framework (the design artifact).
Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.	This research relies on proven methods in Design Science field, like works from Hevner et al. or Wieringa in order to construct a framework that considers both organizational requirements (discovered through interviews) and existing recommendations (discovered through literature review).
Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	It is already in the key goals of the final framework to be consistent with current cybersecurity disclosure obligations and business requirements.
Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The designed framework is presented to the organization that is looking for new disclosure procedures. In the future, the findings will be communicated more widely to other companies that have shown interest in the subject.

Table 6: Design-Science Research Guidelines

B

CONFLICTING LEGAL REQUIREMENTS DUE TO MULTIPLE JURISDICTIONS

Figure 15, proposed by *Information Security Forum* [17] illustrates the problem of a company that operates across multiple jurisdictions:

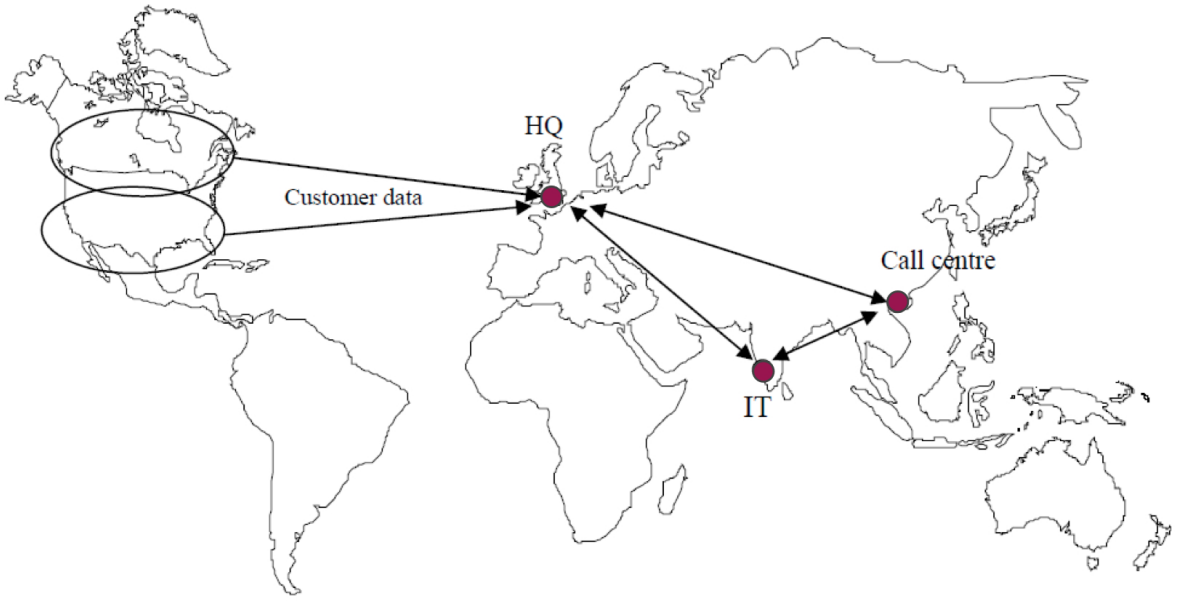


Figure 15: Organisational Operations Across the Globe. Derived from [17].

Assume that a company's Headquarters is located in UK, but it is operating with personal data of U.S. and Canadian citizens. The IT facilities are outsourced to India, and a call center is located in Hong Kong. Such organization will have to deal with multiple legislative regimes of mentioned countries:

"In terms of applicable jurisdiction, the privacy laws of Canada, the USA (of all states where the organization has customers) and the UK are all applicable and should be complied with by the organisation. India currently has no enacted privacy laws (although these are planned), but in order to meet the EU privacy requirements, the organization must ensure that the Indian IT outsourcer complies with EU standards. The Far East call centre will be similarly required to comply with EU standards, while local laws may also be in effect. Hong Kong for example has a series of privacy laws. As the call centre is located in Hong Kong, then there may also be cryptographic export restrictions in force, as well as local obligations regarding certification authorities." [17]

Table 7 illustrates some remarkable data breach notification laws around the globe, derived from RSA report *"A New Era of Compliance"* [16].

YEAR	COUNTRY	DATA BREACH NOTIFICATION LAWS
2003	U.S.	California's landmark SB-1386 sets off wave of state laws
2003-2010	U.S.	46 states enact notification laws
2008	UK	Information Commissioneris Office issues a best practice guidance requiring notification
2009	EU	e-Privacy Directive amended to include notification requirements for electronic communications sector
	Germany	National privacy law amended to include notification
2010	Austria	National privacy law amended to include notification
	France	Draft legislation passed in Senate would make notification mandatory
	Canada	National privacy law amended to include notification
	Mexico	New privacy law enacted that includes notification
	Ireland	Code of Practice issued regarding notification
	Hong Kong	Privacy Commissioner issues guidance note on breach notification
	EU	Data Protection Directive under review for revision; proposed law to include notification requirements for all industries; to be implemented in all 27 EU member countries

Table 7: Data Breach Notification Goes Global

C

NOTICE CONTENT

The notice to affected parties should include the following elements [60, 64]:

- a brief description of what happened. (Who attacked you? When did it happen? How did it happen? How widespread is this incident?)
- if an incident involves personal data, a description, to the extent possible, of the types of data (e. g., full name, data of birth, SSN, home address, etc.)
- a brief description of steps a company is taking to investigate the incident, to mitigate harm, and to protect against any further similar occurrences.
- contact procedures for people willing to ask for additional information (e. g., a toll-free number, website, postal address, etc.)
- steps individuals or other third parties should take to protect themselves from the consequences of the incident (e. g., from identity theft, in case of personal data leak).

D

TOOLS AND RESOURCES FOR INCIDENT COMMUNICATIONS

National Institute of Standards and Technology (NIST) provides a good overview of tools that are required in the company to establish effective incident communications [64].

- Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, email addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity;
- On-call information for other teams within the organization, including escalation information;
- Incident reporting mechanisms, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously;
- Issue tracking system for tracking incident information, status, etc;
- Smartphones to be carried by team members for off-hour support, onsite communications;
- Encryption software to be used for communications among team members, within the organization and with external parties; software must use a FIPS-validated encryption algorithm;
- War room for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed;
- Secure storage facility for securing evidence and other sensitive materials.

E

INTERVIEW OULINE AND QUESTIONS

E.1 GENERAL INTERVIEW OUTLINE

1. *Introduction.*
   - About me;
   - My research within KPMG ICT Security and Control unit;
   - My goals of the interview.
2. *Overview of the coordinator's role in incident management. (Questions varied depending on the coordinator).*
3. *Dealing with internal stakeholders.*
   - In case of an incident, how the incident response group is organized? What are the main players?
   - How communications are established between employees handling the incident?
4. *Dealing with external stakeholders.*
   - In what cases external stakeholders would be notified? When?
   - What would be the main drivers for a company to disclose cyber incident information to external parties?
5. *Advantages and disadvantages of the current approach.*
   - Is there any problems associated with current procedures on incident information disclosure? If yes, what?
   - What do you consider as an advantage of the current approach, what proved to be a good decision to implement for effective notifications?

E.2 QUESTION EXAMPLES TO THE COORDINATORS

Example questions for the incident coordinator:

- What types of incidents are you dealing with?
- Is there specific approach for cyber incident response in particular?
- What are the biggest cyber security threats for the company? (e.g. personal data breach, operational disruptions, etc)

Example questions for the surveillance coordinator:

- What is an approach for information sharing on cyber incidents within a company?
- In which cases cyber incident information is shared externally?
- Does the company cooperate with third parties to achieve better cybersecurity defense?

Example questions for the compliance coordinator:

- Have the company experienced a security breach that has required public notification?
- If so, what was the most substantial impact on the company from a public notification of a security breach? If not, what would possibly be?
- Does the public notification requirement increase the company's willingness to engage law enforcement or other regulatory agencies for assistant in responding to the security breach?
- How does the company's willingness to share changes if no regulations exist that require notification for a particular type of incident (like cyber security incidents), but only guidance that advise to do so?

Example questions for the IRM Strategy and Planning coordinator:

- What does the company want to achieve with its disclosure strategy? What are the main goals?
- Are there any specific issues the company faces when treating cyber security incidents?
- What are the usual timings of incident information disclosure to external parties? For how long the company can delay notifications?

F

POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

National Institute of Standards and Technology (NIST) provides the potential impact definitions for each security objective – confidentiality, integrity, and availability. [68]

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Figure 16: Potential Impact Definitions for Security Objectives. Derived from [68].

BIBLIOGRAPHY

[1] World Economic Forum. Global Risks 2012, 2012. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf.

[2] ISF. Threat Horizon 2014: Managing risks when threats collide, February 2012. https://www.securityforum.org/downloads/documentview/6024.

[3] Gregory E. Shannon. Cybersecurity: Threats to Communications Networks and Public-Sector Responses. Technical report, Software Engineering Institute, Carnegie Mellon University, March 2012. http://republicans.energycommerce.house.gov/Media/file/Hearings/Telecom/20120328/HHRG-112-IF16-Wstate-GShannon-20120328.pdf.

[4] Internet Security Alliance (ISA) and the American National Standards Institute (ANSI). The Financial Management of Cyber Risk, 2010. http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf.

[5] PWC. Cyber crisis management: A bold approach to a bold and shadowy nemesis, August 2011. http://www.pwc.com/en_US/us/forensic-services/publications/assets/cyber-crisis-management.pdf.

[6] Deloitte. Cyber crime: a clear and present danger. Combating the fastest growing cyber security threat, 2010. http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf.

[7] Eric Engleman and Chris Strohm. Cybersecurity Disaster Seen In U.S. Survey Citing Spending Gaps, 2012. URL http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html. Date of publication: January 31, 2012.

[8] PWC. Cybercrime: protecting against the growing threat. Global Economic Crime Survey. White Paper, November 2011. http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf.

[9] Verizon. 2012 Data Breach Investigations Report, 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

[10] PWC. 2012 Global State of Information Security Survey, 2012. http://www.pwc.com/gx/en/information-security-survey/index.jhtml?WT.ac=vt-giss2012.

[11] Kenneth Geers. *Strategic Cyber Security*. Handbooks in Communication and Media. CCD COE Publication, June 2011. ISBN ISBN 978-9949-9040-7-5. URL https://media.defcon.org/dc-19/presentations/Geers/DEFCON-19-Geers-Strategic-Cyber-Security-WP.pdf.

[12] W. Timothy Coombs. Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. *Corporate Repuation Review*, 2007.

[13] Kathy R Fitzpatrick and Maureen Shubow Rubin. Public relations vs. legal strategies in organizational crisis decisions. *Public Relations Review*, 21(1):21 – 33, 1995. ISSN 0363-8111. doi: 10.1016/0363-8111(95)90037-3. URL http://www.sciencedirect.com/science/article/pii/0363811195900373.

[14] R.L. Dilenschneider and Richard C. Hyde. Crisis communications: Planning for the unplanned. *Business Horizons*, 28(1):35 – 38, 1985. ISSN 0007-6813. doi: 10.1016/0007-6813(85)90035-7. URL http://www.sciencedirect.com/science/article/pii/0007681385900357.

[15] Robert Chandler. Message Mapping. How to Comunicate During the Six Stages of a Crisis, 2009. http://go.everbridge.com/crisislifecycle.html.

[16] RSA. A New Era of Compliance. Raising the Bar for Organisations Worldwide., October, 11 2011. http://www.rsa.com/innovation/docs/CISO_RPT_1010.pdf.

[17] Security and Legislation. Complying with information security-related legislation. White Paper, October 2005. https://www.securityforum.org.

[18] Disclosures 2012: Level of cyber-security risk disclosures varies after new SEC guidance, 2012. URL http://blogs.reuters.com.

[19] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design Science in Information Systems Research. *Management Information Systems Quarterly*, 28(1):75–106, 2004. URL http://www.hec.unil.ch/yp/HCI/articles/hevner04.pdf.

[20] Kevin Overcash. Modern cybercrime. *THE ISSA Journal. The Global Voice of Information Securty*, October 2005.

[21] KPMG. Shifting viewpoints. A nuanced perspective on cybercrime, 2012. http://www.kpmg.com/NL/en/Issues-And-Insights/ArticlesPublications/Documents/PDF/Risk%20Consulting/Shifting-viewpoints.pdf.

[22] PWC. Getting real about cyber threats: where are you headed?, June 2011. http://www.pwc.com/us/en/industry/utilities/assets/getting-real-about-utilities-infrastructure-cyber-threats.pdf.

[23] Peter Sommer and Ian Brown. Reducing Systemic Cybersecurity Risk. Technical report, January 2011. URL http://www.oecd.org/dataoecd/57/44/46889922.pdf.

[24] Margaret Rouse. Cybersecurity definition, 2010. URL http://whatis.techtarget.com/definition/cybersecurity.html. This is an electronic document. Date retrieved: April 3, 2012. Date last modified: November 30, 2010.

[25] William T. Shaw. *Cybersecurity for Scada Systems*. PennWell Books, 2006. ISBN 1593700687. URL http://books.google.com/books?id=EyZVJ8KI8C0C&pgis=1.

[26] J. Cebula and L. Young. A Taxonomy of Operational Cyber Security Risks. Technical Report CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tn028.cfm.

[27] Stacy Jordan. Mining gold... A primer on incident handling and response. Technical report, SANS Institute, 2007. http://www.sans.org/reading_room/whitepapers/incident/mining-gold-primer-incident-handling-response_32818.

[28] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Potomac Books, Inc., 2009. ISBN 1597974234. URL http://books.google.com/books?id=cj8FUPKipzAC&pgis=1.

[29] Steven Levy. *Hackers: Heroes of the Computer Revolution*. Penguin (Non-Classics), 2001. ISBN 0141000511. URL http://www.amazon.com/Hackers-Computer-Revolution-Steven-Levy/dp/0141000511.

[30] Michel J.G. van Eeten and Johannes M. Bauer. Economics of malware: Security decisions, incentives and externalities. OECD Science, Technology and Industry Working Papers 2008/1, OECD Publishing, May 2008. URL http://ideas.repec.org/p/oec/stiaaa/2008-1-en.html.

[31] US-CERT. Cyber Threat Source Descriptions. http://www.us-cert.gov/control_systems/csthreats.html.

[32] Vincent Capasso. Top Cyber Security Trends, Breaches, and Observations, 2011. URL http://www.myitview.com/security/top-cyber-security-trends-breaches-and-observations. Date of publication: September 19, 2011.

[33] Security and Defence Agenda (SDA). Cyber-Security: The vexed question of global rules. White Paper, February 2012. http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf.

[34] Tobias Walk. Critical IT-Infrastructure like Pipeline SCADA systems require cyber-attack protection. In *6th Pipeline Technology Conference 2011*, 2011. http://www.pipeline-conference.com/sites/default/files/papers/Walk.pdf.

[35] Robert Lentz. Cyber security maturity model. URL http://www.govware.sg/gw10/dl/01%20Robert%20F%20Lentz%20Singapore%20presentation.pdf. This is an electronic document. Date of publication: Date retrieved: March 6, 2012.

[36] Agnes Huff. Crisis Communications: External and Internal. In W. TIMOTHY Coombs, editor, *PSI Handbook of Business Security*. Praeger Security International, 2008.

[37] W.T. Coombs and S.J. Holladay. *The Handbook of Crisis Communication*. Handbooks in Communication and Media. John Wiley & Sons, 2012. ISBN 9781444361902. URL http://books.google.nl/books?id=mt0F2LBNPa8C.

[38] Jeffrey B Kaufmann and Idalene F Kesner. The myth of full disclosure: A look at organizational communications during crises. *Business Horizons*, 37(4):29, 1994. URL http://search.epnet.com/login.aspx?direct=true&db=buh&an=9408150706.

[39] Barbara Reynolds and Matthew W. Seeger. Crisis and Emergency Risk Communication as an Integrative Model. *Journal of Health Communication*, 10(1):43–55, February 2005. ISSN 1081-0730. doi: 10.1080/10810730590904571. URL http://dx.doi.org/10.1080/10810730590904571.

[40] Mohammed Hossain and Helmi Hammami. Voluntary disclosure in the annual reports of an emerging country: The case of qatar. *Advances in Accounting*, 25(2):255 – 265, 2009. ISSN 0882-6110. doi: 10.1016/j.adiac.2009.08.002. URL http://www.sciencedirect.com/science/article/pii/S0882611009000315.

[41] Mike Smith, Richard Hunter, and Ken McGee. Opportunities and threats in a world of great transperency. Technical Report ID:G00206564, Gartner, September 2010.

[42] Rob McMillan. Six Decisions You Must Make to Prepare for a Security Incident. Technical report, Gartner, September 2011.

[43] Gary K Meek, Clare B Roberts, and Sidney J Gray. Factors influencing voluntary annual report disclosures by u.s., u.k. and continental european multinational corporations. *Journal of International Business Studies*, 26(3):555–572, 1995. URL http://EconPapers.repec.org/RePEc:pal:jintbs:v:26:y:1995:i:3:p:555-572.

[44] PAUL M. Healy, Amy P. Hutton, and KRISHNA G. Palepu. Stock performance and intermediation changes surrounding sustained increases in disclosure*. *Contemporary Accounting Research*, 16 (3):485–520, 1999. ISSN 1911-3846. doi: 10.1111/j.1911-3846.1999.tb00592.x. URL http://dx.doi.org/10.1111/j.1911-3846.1999.tb00592.x.

[45] Paul M. Schwartz and Edward J. Janger. *Notification of Data Security Breaches*. Michigan Law Review, Vol. 105, p. 913, 2007. URL http://www.michiganlawreview.org/assets/pdfs/105/5/schwartz.pdf.

[46] Himanshu Khurana, Jim Basney, Mehedi Bakht, Mike Freemon, Von Welch, and Y Butler. Palantir: A Framework for Collaborative Incident Response and Investigation, 2009.

[47] K.M. Moriarty. Incident coordination. *Security Privacy, IEEE*, 9(6): 71 –75, nov.-dec. 2011. ISSN 1540-7993. doi: 10.1109/MSP.2011.164.

[48] Sasha Romanosky, Rahul Telang, and Ro Acquisti. Do Data Breach Disclosure Laws Reduce Identity Theft? *Journal of Policy Analysis and Management*, pages 256–286, 2011.

[49] Kjell Hausken. Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6):639 – 688, 2007. ISSN 0278-4254. doi: 10.1016/j.jaccpubpol.2007.10.001. URL http://www.sciencedirect.com/science/article/pii/S0278425407000695.

[50] Georgia Killcrece, Moira J. West-brown, Don Stikvoort, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. *Computer Security Incident Response*. SEI Carnegie Mellon University, 2003. URL http://citeseer.ist.psu.edu/685827.html;http://www.cert.org/archive/pdf/csirt-handbook.pdf.

[51] Time-line for the diginotar hack, 2011. http://www.networking4all.com/en/ssl+certificates/ssl+news/time-line+for+the+diginotar+hack/.

[52] KPN hacked, who and when warned users?, February 2012. http://securityaffairs.co/wordpress/2489/cyber-crime/kpn-hacked-who-and-when-warned-users.html.

[53] LLC Ponemon Institute. 2010 Annual Study. Global Cost of a Data Breach, May 2011.

[54] NYSE. Final NYSE. Corporate Governance Rules, 2003. http://www.nyse.com/pdfs/finalcorpgovrules.pdf.

[55] the Division of Corporation Finance of the U.S. Securities and Exchange Commission (SEC). CF Disclosure Guidance: Topic No. 2 – Cybersecurity, October, 13 2011. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[56] David S. Alberts and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age (Information Age Transformation Series)*. Cforty Onesr Cooperative Research, 2003. ISBN 1893723135. URL http://www.amazon.com/Power-Edge-Command-Information-Transformation/dp/1893723135.

[57] Craig 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. ISBN 0415871530. URL http://books.google.com/books?id=A6OxK11RFDoC&pgis=1.

[58] Paul Argenti. Digital Strategies for Powerful Corporate Communications, 2011. http://www.europeanfinancialreview.com/?p=2581.

[59] Zhengchuan Xu, Yufei Yuan, and Shaobo Ji. A decision analysis framework for emergency notification. In *Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, HICSS '08, pages 26–, Washington, DC, USA, 2008. IEEE Computer Society. ISBN 0-7695-3075-8. doi: 10.1109/HICSS.2008.16. URL http://dx.doi.org/10.1109/HICSS.2008.16.

[60] Clay Jonson. Recommendations for Identity Theft Related Data Breach Notification. Technical report, Executive Office of the President, Washington, D.C., September 2006.

[61] W. Timothy Coombs. *Parameters for Crisis Communication*, pages 17–53. Wiley-Blackwell, 2010. ISBN 9781444314885. doi: 10.1002/9781444314885.ch1. URL http://dx.doi.org/10.1002/9781444314885.ch1.

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

[63] Mark Burdon, Jason Reid, and Rouhshi Low. Encryption safe harbours and data breach notification laws. *Computer Law and Security Review*, 26(5):520 – 534, 2010. ISSN 0267-3649. doi: 10.1016/j.clsr.2010.07.002. URL http://www.sciencedirect.com/science/article/pii/S0267364910001056.

[64] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer Security Incident Handling Guide (Draft). Technical report, NIST, 2012. http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf.

[65] Peter M. Sandman. Dilemmas in Emergency Communication Policy, 2002. http://www.orau.gov/cdcynergy/erc/content/activeinformation/resources/Dilemmas.pdf.

[66] Horst W. J. Rittel and Melvin M. Webber. Dilemmas in a general theory of planning. *Policy Sciences*, 4(2):155–169, June 1973. doi: doi:10.1007/BF01405730. URL http://dx.doi.org/doi:10.1007/BF01405730.

[67] Roel Wieringa. Design science as nested problem solving. In Vijay K. Vaishnavi and Sandeep Purao, editors, *DESRIST*. ACM, 2009. ISBN 978-1-60558-408-9. URL http://dblp.uni-trier.de/db/conf/desrist/desrist2009.html#Wieringa09.

[68] Computer Security Division. Standards for Security Categorization of Federal Information and Information Systems. Technical report, NIST, February 2004.