Quantifying Cyber security Risks

Chapter · August 2019

CITATIONS
0

READS
2

2 authors:

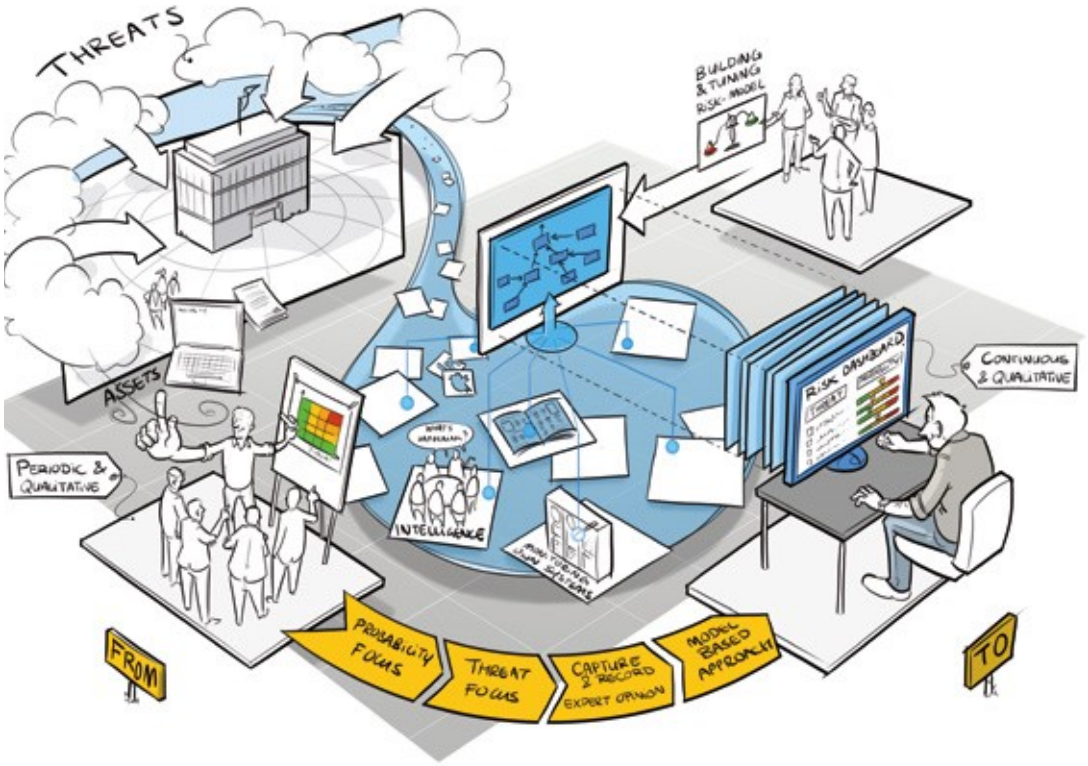
Reinder Wolthuis
TNO
4 PUBLICATIONS **8** CITATIONS
SEE PROFILE

Frank Phillipson
TNO
66 PUBLICATIONS **96** CITATIONS
SEE PROFILE

Quantifying Cyber security Risks

Reinder Wolthuis (TNO), Frank Phillipson (TNO), Peter Rochat (Volksbank), Bert van Ingen (Rabobank), Sander Zeijlemaker (ING), Daniël Gorter (Achmea)

In the financial sector, risk management is one of the key processes in the day-to-day business.



For financial service providers (but also for companies in many other sectors), it is important to understand their risks. Many business decisions are based on estimations of risk and in the financial sector, risk management is one of the key processes in the day-to-day business. Until recently this risk management was mainly focused on financial risks. But currently, financial services rely heavily on electronic channels and complex IT infrastructures, which introduces the risk on cyber-attacks. These attacks might lead to considerable impact on reputation, loss of confidential information or loss of money. This triggered the need for more attention for (cyber) security risk management, a process that is now implemented at all financial providers.

Traditionally, security risk management is a qualitative process based on expert opinion and information at hand; periodically a group of experts gathers, reviews whether the existing risks are still applicable, verifies whether existing risks have correct risk levels, and whether new risks should be added to the list. This usually results in a rather good insight in risks, although not very timely (depending on the periodicity of the meetings), usually formulated qualitatively (e.g. in terms of low, medium, high), depending heavily on expertise of staff that is present during the risk assessment sessions and without a traceable reasoning process. Also, current cyber security risk management approaches usually have an 'asset based' approach, meaning that the risks are established for an asset, such as a process,

a server or a website. As a result, risks cannot be sufficiently related to impact on business processes. These characteristics of cyber security risk management hinder the effective use of cyber security risks in decision making processes.

In the Shared Research Program (SRP) Cyber Security we have developed a quantitative and actual risk assessment methodology, that uses available actual information to quantify risks. The methodology focusses on potential cyber-attacks and their resulting business impact. This leads to a near real-time traceable quantitative risk process, because available information is processed and the risks are automatically updated. The methodology was evaluated against some real-life use cases and in the risk departments of banks. In this article we share these experiences.

Risk assessment

Risk is a metric to estimate the impact of a threat and the likelihood that a threat really leads to this impact. Risk can in its most simple form be expressed as the product of two parameters:

- The likelihood that a threat materializes;
- The impact of a threat when it materializes.

Risk = Likelihood (threat) * Impact (threat)

An example of a threat is a Distributed Denial of Service (DDoS) attack. During a DDoS attack, many computers are used to send large amounts of Internet traffic to one specific target website, with the aim to disturb the accessibility of the website or to even bring it down completely. The potential impact would be that the website owner cannot deliver its services any more through the website and suffers reputational damage and/or financial loss. The likelihood that the threat actually occurs depends on many things, such as the attractiveness of the organization for attackers, the means that an attacker has to generate such an attack, the potential gain that an attacker can make (e.g. by extortion) and the measures that the organization under attack has implemented to mitigate DDoS attacks.

Risk is a metric to estimate the impact of a threat and the likelihood that a threat really leads to this impact.

Risk Quantification

Risks can be expressed in qualitative values or quantitative values. Qualitative risk assessments usually define risks in scales that are expressed in discrete levels such as Low, Medium, High or 1 to 5. Each level in such a scale needs to have a definition that suits the context of the risk assessment, to be able to qualify a risk. This is done both for the impact and for the likelihood of the risk and combined this leads to the actual risk level.
The results of qualitative risk assessments provide a good insight in risks, but there are some drawbacks:

- They depend heavily on the definition of the discrete levels and to really understand risk levels, this definition should also be provided;
- There usually is little distinctive power; i.e. on a scale of 'low, medium, high', most risks will score 'medium', which is not a good base to decide which risks need to be mitigated.

Quantitative risks do not have these disadvantages; they do not need definition tables and usually have more distinctive power because of the theoretically endless number of values it can have.

Estimations for the *impact* of cyber-attacks (e.g. "how much financial loss is caused by a DDOS attack") can be expected to be more-or-less time invariant, provided the IT infrastructure and the various business processes remain the same. However, some impact aspects could very well change over time (such as reputation loss or fines). Usually the impact is quantified by making it financial taking into account costs for response & repair, costs of loss of production time, costs of repairing reputational damage, costs of injuries, cost of fines etcetera.

The *likelihood* of a risk is usually quantified with support of model-based approaches such as Fault/Event Tree Analysis, Attack Graphs/Trees, (Monte Carlo) simulation, Markov Models or Bayesian (Belief) Networks. These models are used to derive the likelihood of a threat, given valid data. Where data is not available, eliciting expert opinion methods can be used. Most methods help to reason in cases of uncertainty and interdependencies (correlated events), which are both hard to perform by humans.

Next to these model-based approaches, current developments in AI, such as Deep Learning, also offer possibilities in threat identification and risk quantification. Here, data is analyzed and models are trained to recognize anomalies in static and dynamic situations. However, here the explainability or traceability lacks.

Building a usable quantified Risk Assessment methodology

The methodology that we have developed is based on the following design parameters and design decisions.

1. We have chosen to develop a methodology that quantifies the likelihood part of a risk. The likelihood part is usually not time-invariant, it could change fast and frequent and we expect that we can use available information to track this change in an automated way;
2. We have chosen to take a threat based approach (contrary to e.g. an asset based approach). This means that we build the model based on a threat that could lead to a certain (defined) business impact (e.g. DDoS attack, identity theft);
3. We have chosen to take a model based approach. We model the processes, infrastructure, the attacker and other assets that are related to the threat. We also include the mitigating measures in the model, that will influence the likelihood of the threat actually leading to business impact;
4. We have chosen for a model that is able to structurally capture and record expert opinion in a transparent way. In this way, we can always trace back why the model was built in a certain way and revise the model when changes (internally or externally) occur.

Based on the points above, we have decided to use a Bayesian Belief Network (BBN), which enables reasoning with uncertainty. It translates uncertainties in threats, effectiveness and availability of protective measures into probability that a certain target is affected.

The developed methodology uses a model and threat based approach and quantifies the likelihood part of risk.

Bayesian Belief Networks

A Bayesian Belief Network (BBN) is a probabilistic graphical model that represents a set of random variables and their conditional dependencies. In the context of the risk methodology, for example, the random variables of interest will be: threats, measures, impact, etc. One of the advantages of a Bayesian network is that these relations do not have to be deterministic. The uncertainty in different threats and in the effect of measures can be modelled. The sensitivity of critical decisions can be evaluated and different scenarios can be analyzed.

In a BBN several types of nodes can be distinguished (see Figure 1). Each node may have multiple states.

- Input (or: Root): nodes with only outgoing arrows. An input node needs as input a definition of states it can be in and the probability of occurrence of each of these states. An input node can be fed by an automated or a manual stream of information that influences its state and by that, through the Intermediate nodes it is connected, influencing the state of Result nodes;
- Intermediate: nodes that are located on the inside of the network and that have one or more incoming arrows from ‘parent’ nodes and one or more outgoing arrows to other Intermediate nodes or to End nodes; These nodes need as input a definition of states it can be in and the probability that it will be in each of the states, given the state of the parents, in the form of a probability table.
- Result: nodes with only incoming arrows, which represent the final result. These nodes need as input a definition of states it can be in and the probability that it will be in each of the states, given the state of the parents.

The way that information or incoming arrows influences the states of a node needs to be defined in the probability tables. Elicitation of the probability tables can be done by using evidence or expert opinion, who has to quantify its belief. A method for this can be found in [Cooke] and [Wisse].

The foundation of the methodology is a Bayesian Belief Network (BBN), which translates uncertainties in threats, effectiveness and availability of protective measures into probability that a certain target is affected.

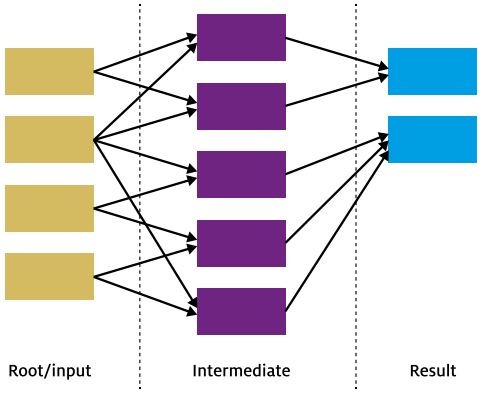


Figure 1: Types of nodes in a Bayesian Belief Network.

The Quantified Risk Methodology

Below the methodology for Quantified Risk management is described, inspired by the 'Business continuity response-recovery chain' in [Phillipson] and the threat and model based approach of [Phillipson2]. In each step, we apply the methodology on a threat example, in this case a DDoS attack (as was done in the Proof of Concept).

Step 1. Identify the threat and the business impact to be modelled

In this step, the threat needs to be described as detailed as possible. Also the business impact needs to be defined: what does it encompass (regulatory fines, service disruption, etc.) and which levels can be distinguished (business impact still is defined as qualitative discrete levels).

The example is built around a DDoS threat. There are many types of DDoS threats (network level, application level, flooding etc.). We have narrowed the example down to a 'Network level DDoS attack'. Please note that we need to build a model for each type of DDoS attack that is applicable in this context. In this case, the business impact is on consumer bank transfers (retail banking) and we have defined three levels of business impact:

- No impact – non-measurable impact;
- Medior impact – 50-100K euro costs, disruption 1-4 hours, medium reputation damage;
- Major impact – over 100K euro costs, disruption > 4 hours, major reputation damage.

Step 2. Identify the business processes and assets that are involved in the attack.

In this step, all the business processes that will be impacted by the defined threat need to be listed, including the major assets. We need to go into a certain detail, but not too much detail, because then the model will become too complex.

In the example of a 'Network level DDoS attack' we have identified the following business processes and assets: Payment service, SEPA transaction service, Other necessary services (needed for the payment process to function), Operating system, Application, Network.

Step3. Identify the mitigating security measures that are in place

In this step, all security measures that are in place that can reduce the probability that the threat leads to impact need to be listed. Also here, it is necessary to go into a certain level of detail, but not too much detail.

In the example of a 'Network level DDoS attack', some examples of potential mitigating measures are: Mitigating business measures, Incident response (on three levels), Testing and training (of incident response teams and processes), External DDoS mitigation (by an external service provider), Attack traceback (the ability to gather information on the source of attack etc.) and Forensics and prosecution. For the full set, see the model in the picture of the model (Figure 2).

Step 4. Identify the actor, its motivation and the means that are available

In this step, the threat actor is defined in a BBN node. It can also be useful to define the actor motivation, the means that an actor has available to launch the attack and the country of origin of the actor.

In the example of a 'Network level DDoS attack' we have identified the following nodes:

- Actor (script kiddy, activist, state sponsored and criminal);
- Actor motivation (extortion, competitor, environmental and/or reputational, thrill seeker, national conflict);
- Country of origin of the actor/attacker (EU, Eastern Europe, Middle East, USA, other);
- Available botnet capacity (the DDoS capacity through botnets available for the actor).

Step 5. Build the model in a BBN

In this step, the nodes are modelled in the BBN, and their interrelationships are determined (by means of connecting arrows).

Step 6. Define the probability tables with relevant experts

In this step, the probability tables are defined. To do this, experts and information are needed to define the dependencies between threats and mitigating measures. Also experts and information are needed to understand the actors and their motivation. It is crucial, for traceability, to record the motivation for the values in the decision table. This can be done in a 'decision table document'.

In the example of a 'Network level DDoS attack' we have made a decision table for the node 'DDoS duration' (see Table 1, that shows part of a decision table), with incoming nodes 'available botnet capacity' and 'actor':

The motivation for this table is that the probability that a long during attack occurs will increase with increasing botnet capacity and with increasing experience of the actor. We define a probability of 0% that there will be a duration of more than 4 hours (H4_PLUS) if the botnet capacity is low.

We now have established the following model of a 'Network level DDoS attack' (see Figure 2)

Experts and information are needed to define the dependencies between threats and mitigating measures.

Actor	Script kiddy				Activist				State sponsored			
Available botnet capacity	Hi	Av	Lo	None	Hi	Av	Lo	None	Hi	Av	Lo	None
H4_plus	0	0	0	0	0	0	0	0	0,3	0,2	0	0
H4	0,3	0,2	0,1	0	0,3	0,2	0,1	0	0,3	0,2	0,2	0
H1	0,7	0,8	0,9	1	0,7	0,8	0,9	1	0,4	0,6	0,8	1

Table 1 – Partial decision table for the node DDoS duration in the model for network level DDoS attack

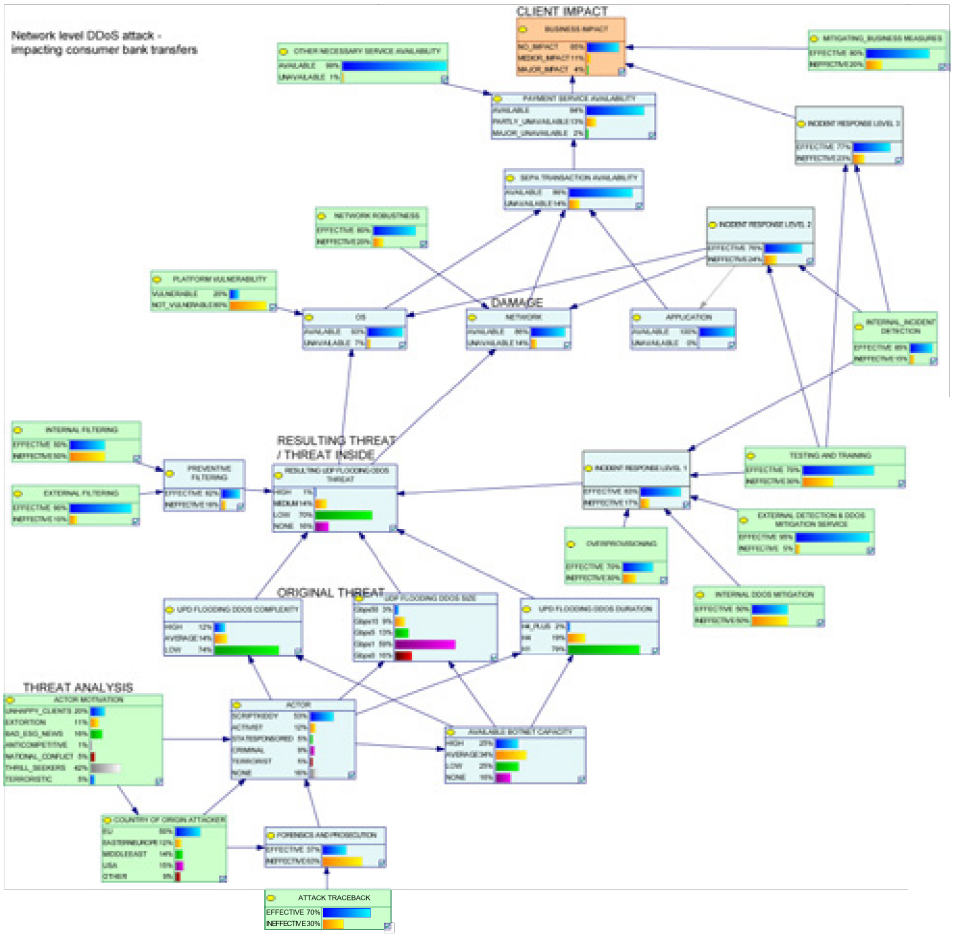


Figure 2: Model of a Network level DDoS attack.

Step 7. Establish the information that is available to feed into the model

In this step we assess what information can be used to feed into the input nodes (the green nodes in Figure 2) and that will influence the probability table of the input node. This information can be acquired internally (e.g. output from technical systems such as log files or service level reports from suppliers) or externally (cyber threat intelligence sources, reports from national certs, etc.). A translation table needs to be defined, that translates the value of the information sources into probability percentages of the input node. The higher the refreshment rate of the information, the more actual the probability table of the input parameter.

If no (structural) information sources can be found, the probability for an input node needs to be determined by experts in which case it is important to record the considerations of the experts.

Step 8. Develop automated scripts to feed the information in the model

Manually updating the information in the model can be tedious, in particular when it contains a lot of input nodes and/or many information sources. To increase the usability of the model, automated scripts can be developed that overtake this task.

Step 9. Put it into operation

After the model is finalized, the information sources and translation tables are established and optional automation has been implemented and tested, the model can actually be used. It is recommended to, e.g., perform a yearly verification step on the probability tables with experts.

The output of the model can be used in the Risk Management process. But the model can also be used for many different analysis purposes e.g.:

- Scenario analysis: a particular situation is simulated by determining a set of multiple input variables and propagation. What answer does that give in the outcome variable(s)?
- Sensitivity analysis: what effect does varying one input variable have on the outcome variable(s)? E.g. what if the effectiveness of our external mitigation provider decreases?
- Root cause analysis (in case that an attack actually occurred): what has caused the observed state of the outcome or intermediate variable(s)?

The model can also be used for analysis purposes, such as root cause analysis and sensitivity analysis.

Lessons learned and outlook

We have gained many useful insights in building the methodology and conducting a Proof of Concept with it:

- Although it takes considerable effort to implement a model for one threat, the effort seems to be well spent because it provides useful new insights. The model and decision tables will most probably not change heavily over time, so the result of the effort can be used for a longer period. Also, this method ensures that expert opinion is structurally recorded and traceable, making it less depending on (presence of) specific experts;
- The actuality of the output of the model (probability of impact when a threat materializes) depends heavily on the actuality of information sources. But even if the information does not change frequently and the model therefore remains relatively static, the model is useful because of the quantified risk level and the knowledge that is recorded in the model;
- Different appearances of one threat-group (e.g. DDoS attack) should be modelled separately. This seems tedious, but for one group of threats, a large part of the model will be the same for all appearances (only some nodes will be specific for an appearance) and many information sources and decision tables can also be re-used;
- One of the challenges was to collect relevant information sources, that are also available when needed. This will remain to be a difficult task, because the information needs to be collected from different parts of the organization and, probably, also externally;
- Also challenging is the translation from information to probability. We have experienced that it helps to define translation tables in terms of maturity levels (is it a one-off, it is done more frequently, is it described, is it structurally done according to the description). But also presence of certain information elements can be used for translation tables (e.g. if we have only 7 of maximum 10 information elements present, we assume effectiveness to be 70%). This needs to be considered from case to case and put into context.

All in all, the method can be well used in practice, both in actual risk management but also for different analysis purposes and we think the effort that is needed to build the models is worth it. As a

next and final step we plan to enhance the methodology and its guidance and automated tooling. so it will become usable for employees in risk management processes.

Our methodology provides traceable, modelled risk estimations based on the current insights. Yet in practice there is an ongoing dynamic dialogue between attacker and defender where both are struggling for the weakest link. The attacker is focused on its exploitation and the defender on avoiding that. This means that both attacker and defender are observing each other and over time they improve their way of attacking or defending based on their observations. This dynamic complex behavior caused by attacker – defender interactions and response of the (resilient) organization [Zeijlemaker], [Zeijlemaker2] will cause the input parameters to increase or decrease over a longer time period. Therefore there is at least a need to do regular risk estimations.

More information

More information and a more detailed description of the model can be found in the white paper 'Quantifying risks' will be published on the SRP cyber security webpage: https://www.tno.nl/srpcybersecurity

Bibliography

[Cooke]
R. M. Cooke, Experts in Uncertainty: Opinion and Subjective Probability in Science, New York, USA: Oxford University Press, 1991.

[Wisse]
B. W. Wisse, N. P. Elst van, A. I. Barros and S. P. Gosliga van, "Relieving the elicitation burden of Bayesian Belief Networks," in BMA, 2008.

[Phillipson]
F. Phillipson, E. Matthijssen and T. Attema, "Bayesian belief networks in business continuity," Journal of Business Continuity & Emergency Planning , vol. 8, no. 1, 2014.

[Phillipson2]
F. Phillipson, I. C. L. Bastings, and N. Vink, "Modelling the effects of a CBRN defence system using a Bayesian Belief Model.", 9th Symposium on CBRNE Threats, Helsinki, Finland, 2015.

[Zeijlemaker]
Zeijlemaker S, 2016. Exploring the dynamic complexity of the cyber-security economic equilibrium, PhD colloquium of the 34th International Conference of the System Dynamics Society, Delft, Netherlands, July 17–July 21

[Zeijlemaker2]
S. Zeijlemaker, 2017, Exploring the dynamic complexity of the cyber-security: does a deeper understanding support financial policy evaluation?, PhD Research Proposal, March 2017, Radboud University

There is dynamic complex behavior caused by attacker – defender interactions which causes the input parameters to change over time.