Evolving From Qualitative to Quantitative Risk Assessment

A Practitioner's Dilemma

It is only recently that quantitative risk for information security has been introduced as a possible evolution from qualitative risk methodologies. Evolving from a qualitative-based risk assessment into quantitative can give real tangible indicators to decision makers, and this transition can be done simply.

While the most prevalent international standards on information risk, the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 R1[1] and the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27005, do not necessarily promote the use of a specific type of analysis, there is a tendency to advocate the use of qualitative assessments as stated in the ISO/IEC 27005 document: "In practice, qualitative analysis is often used first to obtain a general indication of the level of risk."[2] However, there is little evidence that qualitative methods are suitable for managing information risk. As stated by some of its most ardent detractors, the practice of information risk assessment is seriously flawed and represents "the one patch most needed in cybersecurity."[3]

Risk can be defined as "the probability and magnitude of a loss, disaster, or other undesirable events."[4] This definition highlights the concept of probability and loss, both of which are at the core of a quantitative risk assessment.

Introducing the Comparative Analysis

A comparative analysis is provided based on experience working as an information risk manager in a large multinational corporation. The organization, ITCorp (a fictitious name based on a real case), is a large multinational organization designing and selling mass-market IT equipment. The risk management framework for information security was promoted throughout the organization, based upon ISO/IEC 27005, and refers to qualitative indicators.

The risk assessment was performed for a critical system containing a large amount of customer details. The customer relationship management (CRM) system in scope contains up to 60 million records deemed personally identifiable information (PII), including information such as name, address, age, date of birth, gender and product registration number.

Method A: Qualitative Risk Assessment

Once the asset has been identified for the risk assessment, method A follows a typical four-step approach (**figure 1**).

- **Step 1: Business impact analysis**—The risk assessment begins with analyzing the business impact, which, in this case, was rated 4 (high impact) on a scale of 1 (low) to 5 (very high).
- **Step 2: Control assessment**—The control assessment then followed, and it was based upon a predefined questionnaire and covered a wide range of mainstream IT and security controls. The assessment typically contains a list of 71 controls, and its primary purpose is to identify the potential weaknesses of the system in scope.
- **Step 3: Risk analysis**—The risk factors were then derived from the control weaknesses identified in

Figure 1—Model for Performing a Qualitative Risk Assessment (Method A)

Benoit Heynderickx, CISA, CRISC
Is a principal research analyst at the Information Security Forum (ISF). He is the project lead for the ISF's Supply Chain suite of tools and methodologies and a research lead in cloud security matters. Heynderickx is an experienced security risk and assurance professional who has worked across various industries and organizations prior to joining the ISF. While completing his recent master of science in information security and risk, Heynderickx also developed a special interest in the quantitative techniques in risk analysis.

the previous step and rated on a nominal scale of 1 to 5 in terms of likelihood and business impact.

The likelihood was rated according to the expert judgment of the risk assessor and the system owner and based upon the control weaknesses. **Figure 2** shows an example of a highlighted risk.

Figure 2—Example of an Individual Risk Analysis

Risk	Impact	Likelihood	Risk Rating
Unauthorized access from developers into production environment	4	4	High

The risk rating was determined using a risk matrix and, in this case, was rated as high. In total, 11 risk factors identified were rated low to high.

- **Step 4: Action plan**—The action plan was initially developed by the risk assessor and subsequently agreed to by the system owner. When it came time to decide whether to remediate risk 01 vs. risk 03, there was a lack of meaningful data for facilitating the analysis, especially when most of the risk factors were rated high.

When it comes to a risk assessment of a specific critical IT system, the analysis is purely qualitative. While method A would appear relatively simple to apply, there is little evidence of its benefits and outcome over time.

Method B: Quantitative Risk Analysis

The quantitative method (method B) was applied to the same system in scope to be able to compare with the output of the previously used qualitative method. The quantitative model was built following some of the key concepts given by both Hubbard[5] and the FAIR methodology,[6] following a simple step-by-step approach as presented in **figure 3**.

Step 1: Loss Event

In method B, the loss event was quantified by making use of two important techniques in quantitative risk: calibration and decomposition. Calibration begins with the absurd scenario of, for example, losing the maximum amount by experiencing a data breach. The analyst then refines the initial estimate to obtain a more realistic range, often called the 90 percent confidence interval. Decomposition is used to refine the range intervals. Some wide-range estimates are very often given, such as a loss estimate of US$0 to US$500 million.[7] If such extreme losses were of concern, more analysis would be required to derive different scenarios and different range-of-loss estimates.

During the pilot analysis, the following loss event statements were observed:

- The application manager estimated the loss at US$1 per customer record loss, representing a maximum total loss of US$60 million.
- The security officer referred to the introduction of the EU General Data Protection Regulation (GDPR) with potential fines of US$3 billion.

This was a wide range of estimates, from US$60 million to US$3 billion maximum loss, reinforcing the need for further calibration and decomposition to establish a more realistic range interval of loss events, which was subsequently performed as shown in **figure 4**.

The minimum breach was set at 10,000 records, estimating that any smaller breach would hardly be noticed by the organization; moreover, malicious actors would not go through the trouble of stealing less than 10,000 records. The most likely value of 25,000 records breached, as used in **figure 4**, references to the 2018 *Cost of Data Breach Study: Global Analysis*.[8]

Figure 3—A Model for Performing a Quantitative Risk Assessment (Method B)

Meanwhile, the cost per record was deemed less significant for the higher impact event of a breach of 60 million records. This could be explained by the analysis of the numerous publicized data breaches. Indeed, there has rarely been a case of a megabreach exceeding US$210 million in total costs. This was, for instance, the case of the Equifax breach, in which up to 145 million customer records were stolen, which reportedly cost the company US$240 million.[9] Therefore, the maximum loss event could still be regarded as a high estimate of US$210 million.

Overall, the 90 percent confidence interval for the loss event was estimated with the following range values:

- Minimum: US$1.57 million for 10,000 records
- Most likely: US$3.18 million for 25,000 records
- Maximum: US$210 million for 60 million records

Step 2: Threat Scenario

The use of detailed threat scenarios was required to apply probabilities to the loss event. As a prerequisite to this phase, a description of the system in scope was needed, typically including:

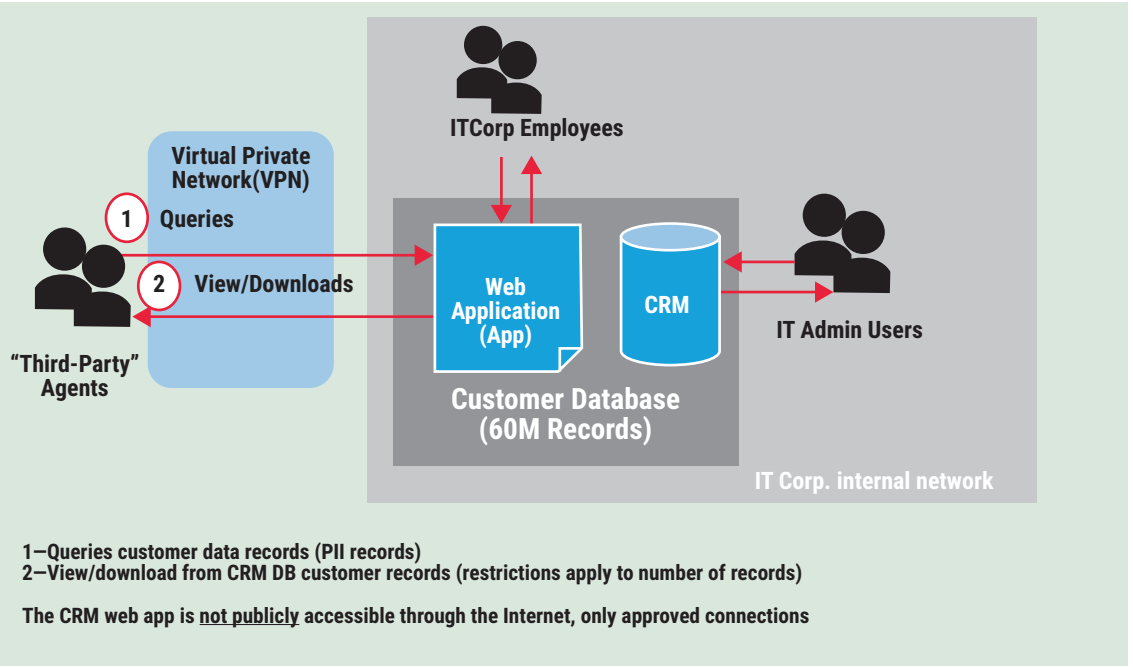
- Data flows
- Threat actors (internal, external, malicious)
- Networking and data center environment

A simple data flow diagram (**figure 5**) was created to better determine the threat scenarios.

Figure 4—Estimates for the Loss Event for the CRM System

	Minimum	Most Likely	Maximum	Comments
Number of customer records breached	10,000	25,000	60,000,000	
Primary response	$8,250	$10,250	$22,000	Minimum 50h – Maximum 400h * US$55/h average cost per employee
Primary replacement	$30,000	$30,000	$50,000	Cost of terminated employee(s) for insider breach; cost of hiring/ training new resources for external breach
Primary cost (1)	$38,250	$40,250	$72,000	
Notification to customers	$10,000	$25,000	$60,000,000	US$1 per customer
Customer support	$10,000	$10,000	$60,000,000	US$1 per customer
Credit monitoring—Insurance	$10,000	$10,000	$60,000,000	US$1 per customer
System downtime	$400,000	$1,000,000	$1,000,000	Cost of halting the system for forensic purposes
Legal	$1,000,000	$2,500,000	$20,000,000	Estimated costs of Equifax breach: US$240M (total)
Public relations	$100,000	$200,000	$20,000,000	Estimated costs of Equifax breach: US$240M (total)
Secondary cost (2)	$1,530,000	$3,775,000	$210,000,000	
Grand total (1) + (2)	$1,568,250	$3,815,250	$210,072,000	Range estimate

Figure 5—CRM Data Flows



In this case, the system in scope was not accessible to the public, and the internal threat was deemed most significant. However, external threats were not dismissed because customer data are always an attractive target to any malicious actors outside of the organization and overall, "there are more [malicious] folks out there."[10]

In total, four threat scenarios were identified and documented as follows:

- **Scenarios 1 and 2**—Internal users access the sensitive PII and extract the data for resell and misuse, applicable for privileged user (scenario 1) or general user (scenario 2).
- **Scenario 3**—Third-party user extracts the data via screenshots for sharing with competitors.
- **Scenario 4**—Hackers access data for financial gain, ideology or espionage.

Step 3: Loss Event Simulation

Each of the aforementioned threat scenarios were then assigned a probability of occurring based upon external research material. For instance, the 2018 *Cost of Data Breach Study: Global Analysis* gave an estimated 28 percent of probability of any type of data breach to occur in the coming two years for any organization.[11] The four threat scenarios were deemed as representative of all possible scenarios that would lead to the event of a data breach, and they were treated as independent of one another.

Based upon this information, it was then possible to derive the threat scenarios as given in **figure 6** introducing probabilities.

For the risk analysis that follows, expected value refers to the probability-weighted average of all possible values, and geometric mean indicates the central tendency or typical value of a set of numbers.[12]

The outcome of the loss event simulation could read as follows:

- There is a 28 percent probability that a loss event would occur within the next two years impacting the CRM system with a range of US$1.5 million to US$210 million.
- The average loss event over the next two years could be estimated at US$51.09 million.
- The most likely value or geometric mean was estimated at US$4.05 million.

Step 4: Action Plan

One proposed action involved the strengthening of controls relating to sensitive user access. If

Figure 6—Threat Scenario and Loss Event Quantification

Threat Actors	Threat Scenarios	Impact-Loss Event Low-High Estimate 90 Percent Confidence Interval	Probability of Loss Event in Next Two Years	Comments
1. IT sensitive users	Extract data for malicious use onto memory drive	US$3.8M – $210M (25,000 – 60M records)	Medium likelihood 10 percent minimum	Direct access to PII; external consultants working as database administrators (DBAs)
2. General users	General user manages to obtain unauthorized higher privileges	US$1.5M – $3.8M (10,000 – 25,000 records)	Low likelihood 5 percent minimum	Little ability to download more than 25,000 records
3. Third parties	Limited access, view only to PII. Possibility to take screenshots with camera phone or similar	US$1.5M – $3.8M (10,000 – 25,000 records)	Medium likelihood 10 percent minimum	Direct access to DB with restricted views
4. External users, hackers, cybercriminals	System intrusion at organization's internal network or third party; lateral movements to gain access to credentials	US$3.8M – $210M (25,000 – 60M records)	Low likelihood 3 percent	Hacker will mostly be interested in larger amounts of data

stronger controls were implemented, this would reduce the range interval for one of the threat scenarios (scenario 1: privileged users). **Figure 7** shows how the average loss event over the next two years could be reduced from US$51.09 million to US$13.86 million. This would represent a significant reduction in the level of risk by improving a small number of IT controls with limited additional costs.

In summary, the proposition for improving the control environment for sensitive users would be cost efficient because it involves simple measures, such as:

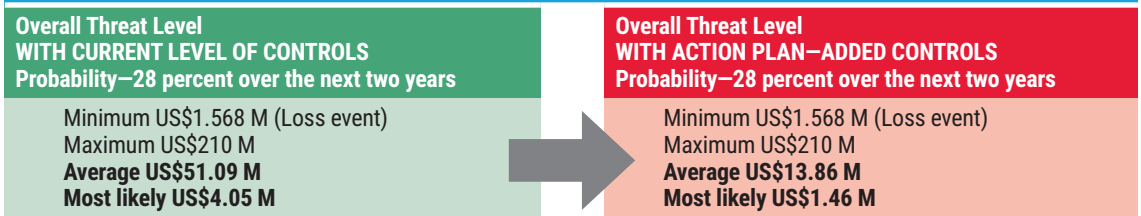
- Tightening of user access, revalidating justification for sensitive user access
- Securing computing environment with lockdown of universal serial bus (USB) ports and restricted Internet access for sensitive users
- Increased monitoring (e.g., security event monitoring) of IT controls for sensitive users
- Regular recertification program

Comparing the Outcome of the Qualitative and Quantitative Methods

The quantitative method involved a larger effort to gather the input data such as the system data flows, incidents and reliable sources of information for past data breaches. Meanwhile, the richness of information given in the quantitative method gave more informed and meaningful information for the decision makers, as opposed to the qualitative method, which relied on intuition and judgments provided by the stakeholders.

The decomposition and in-depth analysis of the loss event was well understood by all stakeholders at the end of the review. In fact, it gave a significant

Figure 7—Average Cost of Data Breach for CRM System and Action Plan



evolution from the qualitative model. With the qualitative method, the business impact was implicitly defined as being high, whereas in the quantitative method, the analysis of the loss event gave a more realistic range interval, providing an interesting and valuable outcome. Most importantly, the use of several financial indicators demonstrated to stakeholders that a rigorous review has been performed to determine a range interval for the loss event.

While the threat scenario focused purely on the data breach, it could be followed up by analyzing more threats such as ransomware or malware affecting the CRM system in scope. In such cases, different input data for the analysis should be considered such as past incident data, and the organization should have such information at hand.

> “A QUANTITATIVE RISK ASSESSMENT PROVIDES A MORE SOUND APPROACH THAT IS RICH IN MEANINGFUL DATA, AS OPPPOSED TO THE LIGHTWEIGHT AND JUDGMENTAL QUALITATIVE-BASED METHOD.”

The loss event simulations only introduced some simple indicators such as average (expected value) and most likely (geometric mean). This was intended to demonstrate that very simple indicators can be used for performing a quantitative risk assessment even though more advanced simulation techniques can be used at this stage, such as Monte Carlo simulations.[13]

Overall, the quantitative method was well accepted because it provided a sound basis for further discussions with the stakeholders, giving them the ability to make well-informed decisions on the action plan.

Conclusion

Risk quantification involving financial indicators and estimates of the potential losses should be clearly communicated to decision makers. Such an approach requires a larger effort in analyzing data from internal and external sources and building simple probabilistic models. Hence, a quantitative risk assessment provides a more sound approach that is rich in meaningful data, as opposed to the lightweight and judgmental qualitative-based method. The additional effort in bringing further quantification is required to improve information risk assessments. Quantitative analysis is used extensively and is proven in many other fields, such as finance, healthcare and insurance, so there is no reason why the same approach cannot be applied to help manage information risk.

Endnotes

1 National Institute of Standards and Technology (NIST), “Guide for Conducting Risk Assessments,” NIST Special Publication (SP) 800-30 Rev. 1, USA, 2012, *https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final*

2 International Organization for Standardization, ISO/IEC 27005:2011, *Information technology—Security techniques—Information security risk management*, 2011, *https://www.iso.org/standard/56742.html*

3 Hubbard, D. W.; R. Seiersen; *How to Measure Anything in Cybersecurity Risk*, Wiley, USA, 2016

4 Hubbard, D. W.; *The Failure of Risk Management: Why It’s Broken and How to Fix It*, Wiley, USA, 2009

5 *Ibid*.

6 Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Elsevier Freedom Collection, UK, 2015

7 *Op cit* Hubbard 2016

8 IBM and Ponemon Institute, *Cost of Data Breach Study: Global Analysis*, 2018, *https://www-03.ibm.com/security/infographics/data-breach/*

9 Hill, R.; “Exposing 145m Equifax Customer Deets: $240m. Legal Fees: $28.9m. Insurance: Priceless,” *The Register*, 27 April 2018, *https://www.theregister.co.uk/2018/04/27/equifax_breach_cost_240m_to_date/*

10 Verizon, *2018 Data Breach Investigations Report*, 2018, *www.verizonenterprise.com/verizon-insights-lab/dbir/2018/*

11 *Op cit* IBM and Ponemon Institute

12 Rumsey D. J.; *Probability for Dummies*, Wiley, USA, 2006

13 *Op cit* Hubbard 2016