Mitigating risk by using communication as a risk control

Explained by the example of a breach of privacy legislation

In today's business world trust is a vital resource for companies. To ensure you do not harm the trust stakeholders place in you as a company, many companies have extensive risk control systems in place. Risk controls ensure predictability, business continuity and an adequate response when incidents occur. However, gaining and maintaining trust is not best achieved through a 'silent' risk management system. Active communications play an essential role in building trust and are a crucial component of the risk management system. When done properly, it can even be a strategic differentiator. In this article we propose that effective internal and external communication play an essential role in managing risk at each stage of the risk lifecycle and that communications should be an integral part of all your risk controls — especially when it concerns how you handle your stakeholders data.

Stakeholder trust gives organisations their license to operate and helps to overcome reputation damage more swiftly. In order to build trust, companies first of all need to behave ethically. But companies also need to be proactively transparent about their behaviour. They need to effectively communicate to stakeholders that they make decisions in their best interest.

Of course this principle applies across a range of topics, nowadays this is especially relevant when you consider how organisations deal with the data that they acquire about individuals. Business' hunger for data is immense. Our article will focus on the value of communications in risk management, using the example of personal data privacy to demonstrate this point. With the internet penetrating our lives further every day, data is the new gold and with all this big data comes big responsibilities. Therefore personal data privacy is a relevant risk topic to demonstrate our hypothesis with. Recently, new European legislation in the form of the General Data Protection Regulation (GDPR) was introduced to govern how organisations should handle personal data. You may perceive GDPR can be seen as a 'hygiene factor'. But we propose a different view. How a company deals with and communicates about data can be a strategic differentiator, according to the Boston Consulting Group it will even boost your financial performance.

8% revenue drop for data misuse

Based on their 'Big data and trust consumer survey,' BCG concludes there is a direct correlation between perceptions of trustworthiness and revenue (related to the use of personal data). They cite up to an 8% revenue drop for companies in the year following perceived data misuse.[1] Furthermore, the results of this survey in 2016 indicate consumers across Europe believe that 48% – 62% of companies are not honest about how they use their data (survey referenced consumers in Italy, Germany, France, Spain & the United Kingdom).[2] The survey also highlighted that consumers feel the information which is provided by companies to explain how and why they use personal data is not presented in a way that is either engaging or accessible to the average consumer.

> *Being mature in Managing Risk and Control implies openly communicating to your stakeholders about the How and Why this is important to you, an even more mature level would be inviting your stakeholders to participate in managing Risk and allow them to actively participate in the process thereof*
>
> — Owen Strijland, Director, Protiviti

Enhancing risk management & uplifting employee engagement

Effective internal and external communication plays an essential role in managing risk at each stage of the risk lifecycle. In our analysis of the risk management lifecycle we distinguish five key milestones: interpreting organisational strategy, considering risk appetite, identifying key risks, designing and implementing controls to mitigate risk, monitoring risk and inevitably managing incidents.

Stage one: interpreting organisational strategy

First it is important to understand what your strategy means. It should be broken down into a set of defined and measurable objectives, which guide day-to-day business. Here, communication has two main purposes:

1. Engaging with stakeholders about your organisational strategy helps bring the outside world into strategic discussions. Ask yourself: how do we want (internal and external) stakeholders to perceive the organisation in general? What do they find important and why?
2. Translating organisational strategy into defined objectives is in itself an act of communication. In order to arrive at a set of business objectives, it is necessary to engage with a range of internal and external stakeholders to determine what is achievable and to make an assessment of the alternative strategies which may be taken to achieve those objectives.

Through the lens of GDPR, organisations must commit themselves to upholding high standards of data stewardship and transparency. The organisation must work with internal and external stakeholders to understand the best way to achieve these objectives. Understanding the best way to achieve these objectives, is only possible when internal and external stakeholders are involved in the conversation. According to the BCG 'Big data and trust consumer survey,' organisations regularly fail to align their privacy initiatives with the expectations of their consumers. The results of their survey indicated that organisations:

- did not communicate how they use their data in a way that they felt receptive to (e.g. using overly legal or technical language in privacy statements);
- fail to use data in new ways that consumers were actually open to (a missed opportunity for innovation); and
- fail to give consumers the power to choose how their data is used.

With this in mind, it is clear that there must be a feedback loop between organisational strategy and key stakeholders to ensure that the strategy is properly defined, the impact on the company's data stewardship is clear and to ensure that goodwill is earned. Note that the BCG survey shows that consumers are willing to share their data with organisations that they trust.

[1] www.bcg.com/en-nl/publications/2017/big-data-advanced-analytics-technology-digital-bridging-trust-gap-how-to-become-trusted-data-steward

[2] www.bcg.com/publications/2016/big-data-technology-digital-bridging-trust-gap-data-misuse

Stage two: identify key risks and consider risk appetite

The next element of the risk management lifecycle is to identify key risks to achieving organisational strategy & objectives and define the appropriate risk appetite. Every organisation should conduct risk alignment workshops at least annually to identify emerging risks and assess the exposure to known risks. Risk alignment workshops should be conducted with internal stakeholders across the business (e.g. Client facing/sales functions, Legal, Finance, Operations, IT) and if applicable external stakeholders. The primary objective of these workshops is clear, however there is an important secondary objective: to create and encourage cross functional dialogue aimed at better understanding the organisation and it's threats, whilst also enhancing cooperation across the organisation.

> *The GDPR enforces a minimum standard of communication. However, these touchpoints with your stakeholders are an opportunity for much more than ticking a compliance box. Effective communication with your stakeholders about how and why you use their data, but more importantly how you will protect their interest, builds company value and gives you greater access.*
>
> — Kate Robinson, Manager, Protiviti

It follows that organisations who are largely dependent on the data they acquire should have repetitive dialogue with their stakeholders to understand the appropriate risk appetite the organisation should maintain.

Stage three: design and implement controls to mitigate risk

Risks identified in the previous stage are the building blocks for your risk control framework. This is the crux of our proposal. We believe that communication is an essential measure for any effective control framework. Below we discuss communication as control, communication in control design and communication as a mechanism for enhancing control effectiveness.

Communication as a control

Proactive communication on topics which are important to your stakeholders is a mechanism for influencing the perception of how the organisation is performing. You should communicate what you are doing to prevent risks (cause) and what you do to limit the impact (effects) when an incident (event) occurs. Within the context of GDPR compliance, the regulation requires ongoing communication with your stakeholders (regulators, customers, employees, job applicants and others). You are obligated to communicate with stakeholders at the point of initial engagement, throughout the engagement lifecycle and in the instance of a data breach or security incident.

These moments of communication are mandatory, however the form and frequency with which you communicate can differentiate you from your competitors. Therefore we urge you to communicate in a clear way about the measures you take to reduce the likelihood of a security incident and how stakeholders can be informed about the management of their data. Now, a security incident at some time is inevitable; the amount of criminal, accidental and political efforts to get to valuable data make this not a question of 'if', but 'when'. Therefore, we suggest that you lay out an approach describing the steps that you will take to remediate and communicate a security incident and share this with your stakeholders. Don't forget to add the steps you expect from your stakeholders. Your stakeholders are wise enough to know that a 100% guarantee is not attainable and we propose that honesty and communication are more effective methods for building and maintaining their trust.

Communication in control design

Creating an effective control framework requires engagement across the business because controls cannot be considered in isolation. For controls to effectively mitigate risk, they must address risk in end-to-end processes. Many organisations rely upon dated or inadequate controls (they are there, so why not?), controls provided by their regulator or controls which are market 'best practice'. However, one size does not fit all and designing an effective control framework requires understanding the underlying purpose of each control. Is a control designed to affect the *cause* (mainly preventative), the *effect* (often a corrective control) or does it simply *monitor* the event (detective control). In a competitive market it is necessary to spend wisely, this means designing controls which are streamlined, precise and time efficient, and at this day and age preferably automated, both in execution as well as in testing its effectiveness.

Consider implementing Privacy Impact Assessment triggers in business change processes. This is an essential step to ensure that any business and IT changes are appropriately assessed for Privacy by Design / Default, reflected in the Record of Processing Activities and assessed for privacy risks. Many organisations struggle to embed privacy triggers because they are to be implemented in often disparate processes, varied across functional areas or locations and lacking consistency. Gathering a complete picture of business change mechanisms and designing controls that properly mitigate these processes requires extensive communication and coordination to ensure that events do not 'slip through the cracks' whilst also not creating burdensome control processes.

Communication as a mechanism for enhancing control effectiveness:

Communication plays a key role in maintaining and enhancing the effectiveness of the risk control framework:

1. *What is the control and how does the control work:* In other words, individuals need to be sufficiently educated on the control framework and how it operates. Those persons who are responsible for executing controls need to be trained on exactly how they should execute the control.

2. *Why is the control important:* Anyone who has worked in the 2nd or 3rd line will be familiar with this situation. A control has failed and the person responsible for executing the control asserts that it doesn't matter because this control is not important anyway. Whether your control framework fails because it was designed poorly or because control owners failed to understand their role in the risk management process does not matter. What is important to recognise is that better communication equals better insight and a greater level of control.

When individuals within the first line fail to understand the importance of their role in regards to risk management and compliance, then they are unable to reinforce the organisations strategic and communication objectives. In contrast, they may undermine the hard work of the organisation by making statements which contradict the organisation's objective. Take for example the scenario where an existing customer contacts your customer service line to enquire about the use of their data or request access to their data. When customer service representatives are not adequately trained, they may fail to answer these questions in an adequate way or they may fail to even recognise that this is a GDPR request. Failure to adequately communicate your control framework and create awareness of individual responsibilities within the framework undermines its effectiveness.

Stage four: monitor risk events

This stage includes the monitoring and analysis of risk events, in other words potential incidents. In general, these efforts go unseen by your stakeholders, they only become aware of this work in the instance that an incident actually occurs. But, you should communicate all of the hard work you do to detect and analyse risk events. This reinforces the messaging that you have created a robust risk management approach, one which has effectively prevented a high volume of risk events from escalating into incidents. In your communication you might indicate that in 2020 you detected 1000 risk events. However, because of your risk and control framework, only 5% of risk events resulted in an incident and of those incidents, none posed a serious risk to the organisation or its stakeholders. Isn't this an impactful message to communicate?

In the context of GDPR compliance, consider communication on suspected data breaches. The regulation enforces mandatory reporting to the Supervisory Authority and to individuals in certain circumstances. However, all organisations still need to identify and assess suspected data breaches, these may relate to employee error, malicious attacks or information security design flaws. Why not communicate to your stakeholders about the number of suspected data breaches your organisation suffered and how your control framework prevented those risk events from escalating into an actual data breach. This creates another opportunity to demonstrate the measure that your organisation takes to protect their data, thereby building trust and goodwill.

Stage five: incident management

As stated above, incidents will happen. You should communicate what has happened, how you are going to deal with it and what you expect from your stakeholders. If you have adhered to our proposed approach, you should already have templated documents and clear communications protocols which are aligned to your strategy of building & maintaining trust. You may consider alternative ways to communicate to stakeholders (via segmentation), you may issue elaborative legal analysis for your regulators and short videos supported by detailed content (in simple language) for your other stakeholders. How you handle this situation is yet another indicator to your stakeholders about how you value their trust and how you will take the measures necessary to protect their interests.

For illustration purposes we refer again to the example of a personal data breach because we feel that this is almost inevitable. In this scenario, you have communicated all of the efforts your organisation has gone to, to prevent a data breach occurring, you have communicated how you would handle a data breach and you have communicated what you would expect from your stakeholders. Now is the moment to put this into action, you should communicate: the nature and scope of the data breach, the steps you are/have taken to fully assess the exposure and to stop or limit the data breach, how you will support impacted stakeholders and what they should do to limit the impact for themselves and the longer term steps you will take to prevent a breach like this occurring in the future.

To conclude

> *Communicating in an open and transparent manner throughout the risk management lifecycle is important to maintain and (re)build trust. This is of course the case when you encounter a crises such as data breaches. However, integrating a clear communication strategy within the risk management lifecycle 1) makes your risk controls more effective, 2) builds trust at any stage, not just when there is a crisis, 3) helps you to distinguish yourself from your competitors and last but not least, when it comes to data, 4) will have a positive impact on your revenue.*
>
> — Kate Robinson, Manager & Owen Strijland, Director at Protiviti

> *In todays world trust is a key strategic asset. We found that actively communicating about Risk Management to stakeholders is a differentiator and could give a competitive advantage if done right.*
>
> — Meeuwes de Ruiter, Senior Communications Advisor & Michel Kok, Founding Partner at HollandSpoor

HollandSpoor helps organisations strengthen their internal and external alignment through corporate communications. We find that corporate communications can only be successful if it is firmly rooted in the organizational strategy and when it is closely connected to the organisations' core processes.

Contacts

Owen R. Strijland
Director, Protiviti
+31(0)20.346.0400
owen.strijland@protiviti.nl

Kate Robinson
Manager, Protiviti
+31(0)20.346.0400
kate.robinson@protiviti.nl

Michel Kok
Founding Partner, HollandSpoor
+31(0)6.5182.6991
michel@hollandspoor.com

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.