Positive risk within cybersecurity

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Positive risk within cybersecurity

Table of Contents

Positive risk within cybersecurity

Greg Bell, Amazon Web Services

Most people think of risk from the negative perspective, such as exposure to loss or managing an adverse event. However, the International Organization for Standardization (ISO) definition of *risk* is the "effect of uncertainty on objectives." In this case, the effect might be positive or negative.

Actual risks might vary between industries, but this standard definition applies to all, and each industry has both negative and positive risks. In the cybersecurity industry, *negative risk* refers to potential loss, and *positive risk* refers to potential gain of assets, knowledge, improvements, or data.

Project management and IT domains have adopted the strategy of evaluating positive risks in business reports and business decisions. However, the cybersecurity industry hasn't yet adopted this as a common practice, and many risk-management methodologies continue to focus on negative risks. If they discuss positive risk at all, it's only briefly.

Traditionally, cybersecurity views risk exclusively through a negative lens. The following are the two common types of negative risk in cybersecurity:

- **Downside risk** – Exposure to loss from external factors, such as a threat. For example, cybercriminals might introduce or increase the likelihood of a security incident.
- **Upside risk** – Exposure to loss while in pursuit of a gain, such as a vulnerability that results from change. For example, when implementing an IT strategy, you might inadvertently increase the potential for a security incident. Upside risk isn't the same as positive risk. Even though it occurs while in pursuit of a gain, upside risk is focused on the potential for loss.

Until recently, cybersecurity has considered only negative risk, and the definition of risk has focused on a potential negative outcome. Positive risks focus on the potential positive outcome at the beginning of risk identification. The exclusion of positive risk results in failure to recognize the positive outcomes in cybersecurity. Because of the focus on negative risk, executive leadership commonly perceives cybersecurity to be reactive rather than proactive and underestimates cybersecurity's contribution to positive business outcomes.

This document defines positive risk for the cybersecurity industry and discusses the benefits and importance of including positive risks within your cybersecurity strategy.

Benefits of positive risk

Especially in an industry such as cybersecurity, which is focused on protecting the business from potential loss, it's easy to frame risk from a negative perspective. Reframing cybersecurity risks based on their potential gains can benefit the business by promoting positive outcomes, increasing the security posture of the organization, and increasing customer trust.

Promoting positive outcomes

Adopting positive risk allows the organization to evaluate and recognize the contribution the domain makes to positive business outcomes. According to Cybersecurity In The C-Suite and Boardroom (Enterprise Strategy Group research report):

- 69% of business and technology leaders believe that cybersecurity is entirely or mostly a technology area with little or no linkage to the business.
- 11% of business and technology leaders equate cybersecurity with regulatory compliance.
- 82% of organizations claim that cybersecurity risks have increased over the past two years due to factors such as increasing cyberthreats, greater integration of technology within the business, and a growing attack surface.

When cybersecurity executives integrate positive risk into conversations and reports, it helps promote the value of secure IT operations within the company.

For example, let's say a business had a data breach several years ago, and the data breach was caused by a lack of a patch management process. The incident is still brought up by the media, and it affects customers' perceptions of and interactions with the company. The business wants to move past the incident and expand their services offerings, but customer trust is blocking sales. Cybersecurity uses positive risk to convince leadership to invest in a patch management process that continually updates applications. The new process dramatically reduces the risk of a data breach, improving the security posture of the company. News of the up-to-the-minute patch management process reaches the media and potential customers. Customers now feel comfortable buying from the business, and sales increase to an impressive level.

Failure to consider positive risks during risk identification can provide an incomplete assessment and affect the business decision. For concrete examples of positive risks that could affect business decisions, see Examples of positive risk.

Increasing security posture and customer trust

Cybersecurity is integral to the security posture of the business. Data breaches can negatively affect customer trust, but a strong security posture and reputation can also increase customer trust and drive business opportunity.

As discussed in Promoting positive outcomes, research shows that executive leadership understands the negative risks associated with cybersecurity but frequently doesn't understand the positive risk, or business value. However, research shows that leadership within cybersecurity understands how a strong security posture can benefit the organization.

In Cyber Security Research: The Innovation Accelerator (Vodafone whitepaper), Vodafone interviewed 1,434 worldwide decision-makers in cybersecurity. According to their data:

- 73% of the respondents believed strong security creates new business opportunities.
- 89% said improvements to their security would increase customer loyalty and trust.
- 90% have also said that they were able to improve their image, to reach new potential clients, and also turn them into actual clients.
- 89% believe that having effective cybersecurity is a relevant competitive advantage, which helps them differentiate from their competitors.
- 24% reported an increase in revenues by using cloud technologies and Internet of Things (IOT) and by adopting targeted IT security controls.

Instead of using potential negative outcomes when communicating with executive leadership, you can also use positive risk to communicate the business value of improving customer trust. Executives can be cautious when funding programs. In some cases, cybersecurity gets the bare minimum needed to operate. Internally communicating positive risks in funding requests can help your leadership understand the business value of cybersecurity. This can result in increased funding for cybersecurity initiatives and drive revenue for the business.

Changing cybersecurity risk language

Part of the challenge of adopting positive risk for cybersecurity is that the technical and domain-specific terminology is focused on negative risk, such as *threats*, *vulnerabilities*, and *security controls*. The cybersecurity industry must evolve and expand its vocabulary to include language that emphasizes the positive business outcomes (or positive risks) that cybersecurity brings to the business. Terms such *business advantage*, *benefits*, and *business value* highlight cybersecurity's contribution to the organization.

Changing the language of cybersecurity helps change the perception that cybersecurity is a technology area focused exclusively on threats and vulnerabilities and that it is untethered from the business. Business leadership commonly underestimates the contribution of cybersecurity to positive business outcomes. For more information about the perception of cybersecurity by leadership, see Promoting positive outcomes.

Increasing adoption in related fields

There is growing interest in many fields for including positive risk because it recognizes the contributions the domain makes to business outcomes. The concept of positive risk has been recently adopted into common project management processes and definitions.

In 2013, the Project Management Institute (PMI) incorporated the definition of positive risk (also called *opportunities*) into the fifth edition of the Project Management Body of Knowledge (PMBOK). PMBOK defines *individual risk* as "an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives." It defines overall *project risk* as "the effect of uncertainty on the project as a whole … more than the sum of individual risks within a project, since it includes all sources of project uncertainty … represents the exposure of stakeholders to the implications of variations in project outcome, both positive and negative."

Unfortunately, PMI's inclusion of positive outcomes in its definitions of risk doesn't apply to the cybersecurity industry yet.

Examples of positive risk

The following are some examples of positive risk for technology, project management, and cybersecurity.

Technology positive risk

One example of a positive risk in technology is that the implementation of a technology could lead to a reduced cost of wages. For instance:

1. Implementing the technology could lead to greater business efficiencies.
2. These efficiencies could lead to reduce labor.
3. Reduced labor could lead to reduced cost of wages.

Project management positive risk

One example of a positive risk in project management is the miscalculation of a project budget could lead to cost savings or funding additional projects. For instance:

1. Implementing a technology project early could result in the project manager miscalculating the project costs.
2. Miscalculating the project costs could lead to excessive project funds.
3. Excessive project funds could lead to cost savings or funding for additional projects.

Cybersecurity positive risk

One example of a positive risk in cybersecurity is the implementation of patch management could increase customer trust. For instance:

1. Implementing patch management could reduce vulnerabilities in the application.
2. Removing vulnerabilities could reduce application risks and make the application more secure.
3. Improved application security could reduce data loss.
4. Reduced data loss could increase customer trust.

Another example of positive risk in cybersecurity is the implementation of incident response could increase employee productivity. For instance:

1. Implementing incident response could lead to detecting increased network traffic.
2. Increased network traffic could lead to detecting employee misuse of resources by accessing content that isn't work-related, such as music and video streaming services. These activities consume network bandwidth and can negatively impact network and application performance.
3. Detection of employee misuse of company resources could lead to blocking these services.
4. Blocking these services could reduce consumption of network bandwidth and increase employee productivity.

Finally, the last example of positive risk in cybersecurity is the implementation of an incident response plan could increase business opportunities and compliance with privacy laws. For instance:

1. Implementing an incident response plan could lead to quickly detecting and identifying malware and ransomware.
2. The identification of malware and ransomware could minimize the impact and mitigate the threat to company resources.
3. Mitigating the threat to company resources could lead to new business opportunities and help the business remain in compliance with privacy laws.

Cybersecurity risk response

The responses to positive and negative risks are vastly different. For negative risks, you take steps to minimize the impact on the outcome, but for positive risks, you take steps to maximize the impact on the outcome. The following table shows potential responses to positive and negative risk.

Risk type	Response	Definition
Positive risk	Exploit	Maximize the probability or likelihood of the risk occurring in order to realize its positive effect.
	Share	Allocate part of the ownership of or responsibility for the risk to another party. This is the same approach as with a negative risk, and it tries to control the potential loss or gain.
	Enhance	Increase the conditions that create the risk in order to maximize the opportunity.
	Ignore	Disregard the possibility of the risk, and take no action. This response is common when the probability of the risk is very low or when the benefits of potential positive outcome are minimal.
Negative risk	Mitigate	Minimize the probability or likelihood of the risk occurring.

	Transfer	Shift responsibility or liability for the risk to another party, such as purchasing an insurance policy to transfer the risk to an insurance company.
	Avoid	Eliminate the conditions that create the risk.
	Accept	Acknowledge the existence of the risk but take no action.

For negative risks, organizations avoid, transfer, mitigate, or accept the risk, based on their risk tolerance and appetite. They try to prevent the risk from occurring, and if it does, they try to minimize its impact on the overall mission.

The best way to illustrate the positive risk responses is to use examples:

- **Exploit** – A security executive learns that a well-qualified security professional has recently decided to seek new employment and arranges a generous signing bonus to entice the prospective employee to his team.
- **Share** – A business unit leader would like to improve security by using a privileged access management product but doesn't have a sufficient budget to purchase the tools and services in the current fiscal year. The leader works with a leader from a different business unit who will purchase and implement the tool as a pilot project and later expand installation to support both business units.
- **Enhance** – An employee has identified an opportunity to automate an existing business process to reduce cybersecurity threats, but it requires an investment in time and equipment. Seeing the positive benefits of such a process, the manager approves overtime labor hours to develop the capability and repurposes existing hardware and software resources that enable the project to proceed.
- **Ignore** – A finance executive learns that an employee working in the sales department has developed a new application that automates a tedious and manual task. The application was recently authorized for use in only the sales department. The finance executive obtains a copy of the new application to gain a similar advantage in his department, without explicit authorization.

Next steps

Technology and project management domains have adopted positive risks into their risk assessment processes, but the cybersecurity industry has historically excluded them. Positive risks can result in positive business outcomes, and the cybersecurity industry must transition to embrace positive risk and realize the benefits.

You can start communicating positive risks immediately in all communications. For instance, risk assessments, security assessments, or status reports should include a section on positive risks. Funding requests to executive leadership should include positive risks, communicate the potential benefits to the business and highlight any potential business advantages gained by approving the request.

FAQ

What is the difference between upside risk and positive risk?

Even though *upside risk* and *positive risk* sound similar, they are actually very different. Within risk, there is either a positive or negative outcome, and within the negative outcomes, there is either an upside or a downside.

Positive risk is the potential gain of assets, knowledge, improvements, or data. For example, you implement patch management and a process to remove vulnerabilities quickly, such as within one week. Over the course of the next year, you have no security incidents.

Upside risk is exposure to loss while in pursuit of a gain. For example, the business deploys a new application, and you implement patch management and a process to remove vulnerabilities quickly, such as within one week. The exposure to loss (the period of time when you remove vulnerabilities) is in pursuit of a gain (a more secure application), so this is considered an upside risk. You can increase the upside risk by changing the process to remove vulnerabilities to one day, or decrease the upside risk by changing the period to one month. Basically, upside risk is the uncertain possibility of gain while trying to minimize a loss.

Why is it important to include positive risk within cybersecurity?

Integrating positive risks within cybersecurity risk assessments and conversations helps promote the value of cybersecurity to the business. For more information, see Benefits of positive risk.

Resources

- Cybersecurity In The C-Suite and Boardroom (Enterprise Strategy Group research report)
- Cyber Security Research: The Innovation Accelerator (Vodafone whitepaper)
- Integrating Cybersecurity and Enterprise Risk Management (ERM) (NIST publication)
- Clarifying "Upside" and "Positive" Risk (FAIR institute blog post)

Document history

The following table describes significant changes to this guide.

Change	Description	Date
Initial publication	—	May 27, 2022