BITSIGHT

EBOOK

# 5 Ways to Evaluate the ROI of Your Cybersecurity Program

Cybersecurity is taking center stage in board meetings and it's putting CISOs and security leaders in the hot seat answering questions from a non-technical executive audience. As executives see more headlines about cyber events and invest more money in their cybersecurity programs, it has them asking their CISOs not just whether their cybersecurity programs are working, but to prove it. While a valid question, the answer requires a lot of context and a fair amount of translation.

This ebook walks through five steps that help CISOs and non-technical executives evaluate their organization's cybersecurity performance from a common and shared perspective.

For the purposes of this eBook, it is critical to understand how Bitsight defines ROI in cybersecurity. Cybersecurity ROI is not about cost savings. Rather, it is about how well your program enables the organization to achieve its goals while managing the associated risks to acceptable levels.

## 5 Ways to Evaluate the ROI of Your Cybersecurity Program

**01** **Reframe what success looks like**

**02** **Establish & understand your cyber risk appetite**

**03** **Assess & quantify risk from a variety of angles**

**04** **Use benchmarking to get perspective on how you're performing**

**05** **Where the business and cybersecurity connect to facilitate continuous improvement**

## 1. Reframe what success looks like

The same interconnectivity that allows us to innovate and advance our businesses today increases our exposure to cyber events. Simply doing business today is a cybersecurity risk. So given the inevitability of cyber events, what should a return on your cybersecurity investment look like?

The role of the CISO and cybersecurity teams is to enable the business to achieve its goals securely, and the measure of success must account for that. A recent Forbes article proposes that ROI can be demonstrated by how much cybersecurity enables the future of the business. Cybersecurity isn't a means to an end itself, but rather a means to successful growth.

Consider that credit rating agencies are now taking an organization's cyber risk posture into account as they evaluate their financial solvency. Does the increasing relationship between your cybersecurity posture and your financial posture change how you evaluate the ROI of your cybersecurity efforts? It should. With this context in mind, you should no longer measure cybersecurity performance with a checklist of technical controls or deem it successful only if all risk is eliminated. Instead, include an understanding of the potential financial impact your current cybersecurity posture creates and mitigates.

This requires a concerted effort to stop isolating cybersecurity from the business. A recent Harvard Business Review article speaks to how translating cybersecurity initiatives into business context is critical to illustrating the effectiveness of a cybersecurity program. Therefore, cybersecurity ROI metrics should be established and agreed upon by the CISO, CFO, and other executives.

For example, a company invests $250 thousand in security training for employees and $2 million in multi-factor authentication to support the shift in remote working. During this time, employees could continue doing their jobs with minimal increases in security vulnerabilities despite the expanded technical landscape. For another example: a company deploys client-side device identification for high risk customer transactions to increase security while minimizing customer impact.

Regardless of how you frame cybersecurity performance, you need to measure it. That requires establishing some KPIs or metrics that enable the CISO to show how security initiatives helped the business grow as securely as possible. Identify and measure your metrics by defining your cyber risk appetite and implementing cyber risk quantification.

For more information on establishing KPIs and metrics, review the Forrester study **"Better Security & Business Outcomes with Security Performance Management."** This study details key methods and metrics for leaders to understand and report performance to leadership.

You should no longer measure cybersecurity performance with a checklist of technical controls or deem it successful only if all risk is eliminated. Instead, include an understanding of the potential financial impact your current cybersecurity posture creates and mitigates.

## 2. Establish & understand your cyber risk appetite

Most organizations are willing to accept some level of risk to achieve their goals. To maintain a healthy balance between cyber risk and business growth, you need to identify and quantify the thresholds that your organization deems acceptable given its business goals. These acceptable thresholds are your organization's risk appetite.

Some organizations have different risk appetite thresholds defined for various business units as well as an overall risk appetite. Defining the overall risk appetite occurs at the board and executive level, and should take into account a variety of factors—including everything from business strategy, goals, regulations, insurance, and cyber vulnerabilities. In fact, Deloitte suggests that boards and executives should have a clearly articulated risk appetite incorporated into existing risk management and governance processes.

It is critical that the CISO also has a seat at that table. To protect and enable the business, they have to provide guidance on the cybersecurity risks related to the organization's business strategy and goals. This enables the executive team to discuss and determine whether the benefits of a certain business strategy outweigh the cyber risk, or vice versa.

The relationship between your risk appetite and cybersecurity ROI is captured in an article from Marsh McLennan that states "an effective, measurable, and actionable cyber risk appetite provides institutions with a risk management capability to set and communicate strategic boundaries for cyber risk-taking across the institution." A risk appetite essentially starts putting cyber risk and cybersecurity into business context and enables all executive stakeholders to better understand the cyber risk implications of new business initiatives, technology, or even human resource policies, like shifting to a work-from-home culture.

> "The challenge for most organizations, however, is defining what "acceptable" means to them.

As an example, consider the increased vulnerabilities that resulted from shifting entire organizations to remote systems after COVID-19 started. Many organizations made the shift rapidly and without preparation for the safety of their employees and for the sake of operations. While that strategic decision enabled them to maintain operations, it also increased the probability for more cyber events as employees were relying on their home networks, which were less secure than their office networks.

The risk appetite discussion here could go something like this: If we shift to remote work to maintain our business and generate revenue, are we willing to accept losses associated with cybersecurity incidents in the amount of $1 million? If not, the CISO and executive team can discuss various risk mitigation strategies that will protect the organization while enabling the business to work from home. They then weigh the costs of those strategies against the probable costs associated with the risk as well as the probable rewards of enabling their workforce to work from home.

The challenge for most organizations, however, is defining what "acceptable" means to them. For many, it is helpful to reframe risk appetite probabilistically. Are you comfortable with a 10 percent chance of losing $1 million in a given year? What about a 30 percent chance? In addition, framing what's acceptable in quantitative figures provides clearer boundaries for the CISO and the rest of the executive team. This not only helps ensure they share a common understanding of the organization's risk appetite, but enables them to collectively establish the appropriate KPIs so CISOs can allocate resources and measure results accordingly.

Then, when it comes to ROI, they can measure whether those risk mitigation strategies were effective at maintaining that balance.

## 3. Assess & quantify risk from a variety of angles

A cybersecurity risk assessment by itself is not a measure of ROI. It is simply a means of understanding your organization's security posture so that you can identify vulnerabilities and create informed risk management strategies. That said, an accurate cyber risk assessment is a crucial component for cybersecurity performance tracking and risk mitigation.

There are a variety of tools and approaches to conducting a risk assessment. Regardless of how you approach it, remember that achieving the most accurate illustration of your risk posture requires assessing a variety of data sources. That means analyzing both insideout and outside-in data sources, as well as going beyond self attested data sources to incorporating validated data sources (such as pulling data directly from your network and systems). This yields the most accurate representation of risk and provides a baseline to monitor from.

Once you have a validated cyber risk assessment, you can begin mapping the cyber risks to your organization's business strategy, and vice versa. This enables you to identify the necessary risks your organization will need to undertake to achieve its goals. From there, you can quantify the potential loss value of those risks and weigh them against the potential growth value of the business initiatives that create or exacerbate the risks.

For example, migrating a legacy on-premise application to the cloud increases loss exposure from certain threats, while also reducing exposure from others. Moving to the cloud also enables greater business opportunity ten-fold. In this case without a "business aware" risk analysis the wrong decision may be made because the greater business context wasn't taken into account.

The key to risk quantification is presenting results on a scale that show a range of probability in terms of likelihood and cost. These ranges help identify outliers and areas that fall outside the scope of your risk appetite, while enabling better risk management discussions with the business. In addition, by presenting the probable financial impact of likely cyber events associated with business activities, you can translate technical cyber ramifications into business terms so the entire executive team is aware of the potential impact of action or inaction.

## 4. Use benchmarking to get perspective on how you're performing

While cyber incidents can happen to anyone, organizations in different industries, geographies, or even different sizes face different risks and ramifications. While it's important to conduct a standalone analysis of your own organization, comparing yourself to other organizations in the same grouping or cohort provides helpful context.

For instance, according to the 2021 IBM Cost of a Data Breach Report, the healthcare industry has had the highest average cost of a breach for the last 11 years with their 2021 average peaking at $9.23 million. In addition, the US, Middle East, Canada, Germany, and Japan have the highest average cost of data breaches for the last two years. Understanding these industry or geographic trends helps you determine what's acceptable in your organization.

Benchmarking also highlights the probability of likely attack methods. If organizations within your industry, geography, or size are more likely to experience certain threats, then your evaluation should focus on whether you have the controls and strategies in place to mitigate those attack vectors. For example, according to Verizon's DBIR 2021, "The Financial sector frequently faces credential and Ransomware attacks from External actors." If your organization is in the financial services industry and your security performance in those areas is weaker than others in your cohort, then you're more likely to stand out to attackers and your probability of a likely event increases.

Using these same benchmarks can assist in prioritizing limited resources and security budget. Understanding how to allocate resources against the most likely threats, and how those compare to the broader sector, can be used to evaluate ROI. Companies that have these capabilities not only understand the financial loss exposure reduced by their spending, but also evaluate the relative priority of their investments. Reducing $100 of loss exposure from the most likely threats in your industry is a higher priority than reducing $100 of exposure from an unlikely event for example.

Finally, tracking and monitoring the trends can help highlight potential regulatory ramifications that could increase the potential cost of incidents. Industry specific regulations are not new, but as more industries fall victim to target attacks, government agencies are releasing regulations, rules and guidelines. For instance, after the Colonial Pipeline attack in early 2021, TSA issued a directive requiring "owners and operators of critical pipelines transporting gasoline or other hazardous liquids are required to take specific security measures to protect against ransomware attacks, develop recovery plans in the event of an attack and review their existing cybersecurity plans." This instance illustrates how trends or critical events can have cyber or financial ramifications on anything from cyber insurance to security controls.

"

If organizations within your industry, geography, or size are more likely to experience certain threats, then your evaluation should focus on whether you have the controls and strategies in place to mitigate those attack vectors.

## 5. Where the business and cybersecurity connect to facilitate continuous improvement

Cybersecurity is an ongoing feedback loop, and this is by no means the final step. Rather, this is a reminder that one thing remains the same in cybersecurity, and that is change. So not only do you need to continuously monitor the threat landscape and your organization's security control performance, but the business and the security teams need to constantly discuss evolving business priorities and challenges to ensure there is continuous alignment on cyber risk probability and likelihood.

That's because cybersecurity and business strategies have a symbiotic relationship. If you pull one lever or change one component on one side, it's likely to affect the other side. This basic tenet is critical to not just understanding your security programs ROI, but also maintaining a healthy balance between cyber risk and business outcomes.

“

That's because cybersecurity and business strategies have a symbiotic relationship. If you pull one lever or change one component on one side, it's likely to affect the other side.

Consider again the remote working example we've been using throughout this eBook. Prior to shifting to working from home, an organization's most likely and impactful cyber risks may have been malware infecting a local workstation and spreading across the network. The security team, therefore, likely prioritized web content filtering and network segmentation to mitigate those risks. Once the organization shifted to a remote workforce, those cyber risks shifted with it. So malware infecting a workstation still poses a financial risk. However, due to the distributed nature of the workforce, the security team will need to not only implement endpoint protection solutions, but also find a new way to prevent infections from a home internet connection that bypasses the corporate web proxy and content filtering.

In some cases, new business shifts can swap out cyber risks, or, more likely, increase the organization's cyber risks. Failing to see the impact that a new strategy has on your security can not only lead to increased vulnerabilities, but also to a false understanding of your security performance.

Remember, cybersecurity isn't about the absence of risk. It is about maintaining a healthy balance of risk with reward that enables the business to perform while cost effectively keeping the probability of risk at an acceptable level.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT