1898 & CO

PART OF BURNS & McDONNELL

WHITE PAPER / **RISK MANAGEMENT PROGRAMS**

Presenting the value of effective risk management

Risk management programs, with business-aligned key performance metrics, demonstrate a return on investment that all executives can get behind. When the chief information security officer of an organization successfully makes a case for the return on investment of a risk management program, the entire organization benefits.

"media media" about="/careers/201
foaf:Document">
media__icon">
/careers/2018/05/get-comfortable-discomfort
encemag.org/sites/default/files/styles/grid_th
etching his arm through a speech bubble" /></a>
body">
class="media__headline"><a href="/careers/20
comfortable with discomfort and start communicating
content="Get comfortable with discomfort
p class="byline">
">Shuai Li</a><time>May. 10, 2018</time></p>

Like all business leaders, chief information security officers (CISOs) are faced with the challenge of demonstrating a return on investment (ROI) for the budget they are allocated each year. This challenge is a struggle for many CISOs attempting to monetize cost savings and investments to compare investments made across the organization, dollar-for-dollar.

Even in a best-case scenario, this approach has a very high likelihood of failure — and backfiring at worst. Risk management programs are not normally designed to generate revenue; therefore, the only dollar figures they present are the associated costs of the program, and costs alone will not win the ROI challenge.

It is possible, however, for CISOs to demonstrate the ROI of a risk management program in ways other than revenue dollars. The secret to such a demonstration is to articulate the key risks your program is addressing in light of the business drivers being protected.

When a CISO effectively describes a program's impact on those same business drivers, that is when the cumulative ROI of revenue generators becomes clear.

By utilizing a three-step process — selecting a framework to set the foundation for a program's structure, creating a risk profile, and identifying mitigating controls for key risks — CISOs will have the tools necessary to present ROI information of a risk management program that meets the needs of the organization and meshes with existing revenue streams.

Choose a framework

The process of demonstrating ROI begins with choosing a framework. Choosing a framework may seem like an odd place to start a process to measure the return generated by a risk management program, but this is an essential first step as it sets the foundation for how the program is perceived by upper management.

> **■ Executive peers do not talk about vulnerabilities, mitigation strategies or zero-trust security architectures. They talk about revenue streams, competitive advantages, innovation and the like.**

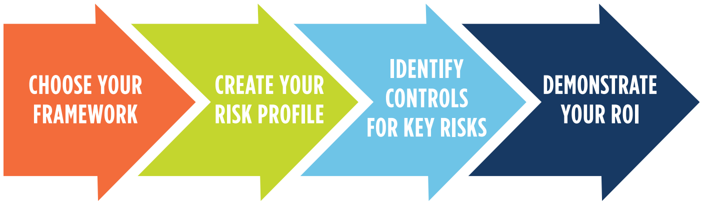

Figure 1: *The steps to presenting an effective business case for risk management program ROI.*

Think of the framework as the lens through which the program is viewed. The chosen framework — NIST, ISO, C2M2, etc. — is not going to impact this process, but choosing a single framework and sticking with it is imperative. Without it, all measurements will be built on a foundation of shifting sand. While the framework does not define the program, it does provide a defined set of reference points.

It is important to note that compliance standards are not frameworks. Compliance requirements establish minimum thresholds for acceptable behavior by or within an organization. They measure effectiveness as a binary decision: Either an organization complies, or it does not. There is no extra credit for exceeding the minimum requirement.

Conversely, a framework describes a risk management program on a continuum of maturity comparing the organization's unique target with its current state with built-in measures for future state as the landscape changes.

Create a risk profile

Understanding and organization's position on taking risks, the kinds of threats that it faces, and the existing risk mitigation investment is just as important as choosing an effective framework. These factors, and others, come together to form the organization's risk profile. There is no one-size-fits-all solution when it comes to risk profiles because each one will be as unique as the organization it is designed to serve.

An organization's risk tolerance represents how willing it is to accept some amount of risk in lieu of taking action to reduce it. Organizations with high risk tolerance tend to spend less on security controls but pay a higher price when a security loss occurs. Conversely, organizations with low risk tolerance will likely spend more money to reduce the likelihood of a security event from occurring. The tolerance level of an organization is highly dependent upon the leadership in place and will usually shift as leadership changes occur at the board of directors or senior management levels. This is one reason why risk management programs often see great change when new leaders step into their roles.

Identifying the risks an organization is likely to face is another key element of the risk profile. It is important to consider many types of risk including technical, geopolitical, societal, environmental and economic. Some scenarios will cross multiple types of risk. For example, consider the recent COVID-19 pandemic, which began as a health risk and quickly gave rise to geopolitical, economic and technical impacts.

For each risk that is identified in the previous step, the task is now to estimate the likelihood and impact of such an event, if it were to occur. The impact must be measured in context of an organization's business operations. This is paramount to effective evangelism of a program and its ROI to the business .

Keeping the risk discussion centered on the impacts to the business will translate security objectives into business objectives with no additional effort.

There are many methodologies available to quantify risk that may be useful tools as an organization matures its risk management program. It is important to set a threshold on how far out an organization will need to consider risks, meaning it is nearly impossible to consider every event that might occur over the next 15 years. Instead, as a program matures, organizations can look further into the future to anticipate potential risks. The risks with the greatest impact and likelihood will then become the key risks that demand attention.

Identify controls for key risks

Armed with a list of key risks, the next step is to identify the controls that help mitigate the likelihood, impact, or both. These controls are the levers that a security leader can pull to maintain the risk posture within the organization's tolerance level. As leadership changes, the control investment can be adjusted to align with the new tolerance level. The key risks to an organization will change over time and the associated control framework will need to be adjusted as they do.

The chief financial officer of an organization may not be familiar with the nuances of a cyberattack against the organization's control systems; however, the financial impact of production facilities going offline for two weeks would be apparent.

If the key risks are based on business drivers, then the key controls represent the security functions that are most vital to protecting the business.

The set of mitigating controls helps to draw a direct correlation between the success and ROI of an organization's risk management program. As key performance indicators (KPIs) are established, the connection becomes even more clear. As such, the KPIs for the key controls are the measures that define how successfully the program is protecting the most critical business functions within the organization.

Demonstrate ROI

Demonstrating the ROI of a risk management program will change the way other executives in the organization look at the security function. Instead of being another back-office expense, the program can instead take its rightful place as a business enabler .

For a long time, security executives have either accepted being perceived as an extension of the IT department or made attempts to demonstrate their financial value purely through the avoidance of a costly security breach — a risk no organization can avoid forever.

Articulating key risks by focusing on the impact those risks will have on business drivers will define a program in terms that other executives care about. Few executives will understand or be concerned by malware introduced through watering hole attacks or expired domain certificates. The ROI that everyone will understand will be rooted in the value of the risk reduction achieved through the key controls .

Without the controls in place, there is an increased likelihood that the financial gains of those business functions would be reduced or eliminated. A factor of the gains then should be applied to the enabled revenue of the risk management program.

Over time, just as revenue-generating functions must show progress, so should the security leaders. Showcase progress against the KPIs that are protecting the business to demonstrate the increased scale and/or reduced cost of those controls per revenue dollar generated. There are several ways to demonstrate continuous improvement, but these methods should always be produced through the organization's KPIs to maintain focus on the business being enabled.

The ROI measurement draws on the value of the business being protected by the key controls.

Conclusion

CISOs, like all other executives, are being challenged to show year-over-year increases in the ROI of their programs. While it can appear daunting, there is a proven path to measuring the ROI of your program in financial terms. By selecting a framework to set the foundation for your program's structure, creating a risk profile, and identifying mitigating controls for key risks, CISOs have all the information needed to populate the ROI formula.

As an organization's program matures, it is important that a watchlist of risk profile movements be maintained and that the CISO is willing to shift focus as the business changes. This keeps a program aligned with key business drivers over time and keeps the CISO at the table with other leadership. A finely tuned risk scorecard can eventually begin to identify business risks before other departments identify them. And when that happens, the CISO has succeeded in really elevating the role to that of a chief risk officer.

Selecting the right KPIs makes all the difference.

The key performance indicators used to record and report the effectiveness and ROI of a security program will make all the difference in changing the perspective of other executive leaders. The object is to create KPIs that clearly communicate the value of the business functions that are being protected. Wherever possible, keep the KPI definitions in positive language. For example:

- **IT:** System uptime vs. downtime.
- **Manufacturing:** Number of widgets produced vs. lost production time.
- **Utilities:** Number of units served per customer vs. customers without service.
- **Hospitality:** Revenue earned vs. lost.
- **Industrial:** Days without a safety incident (due to system resiliency failure).

About 1898 & Co.

1898 & Co. is a business, technology and security solutions consultancy where experience and foresight come together to unlock lasting advancements. We innovate today to fuel your future growth, catalyzing insights that drive smarter decisions, improve performance and maximize value. As part of Burns & McDonnell, we draw on more than 120 years of deep and broad experience in complex industries as we envision and enable the future for our clients. For more information, visit **1898andCo.com**.