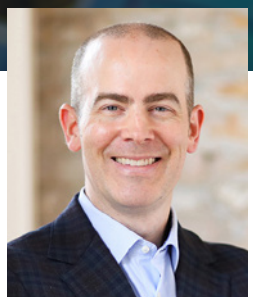
Aligning Cybersecurity Risk with Business Imperatives

OCTOBER 2021

by Luke Tenery and Ross Rustici



Luke Tenery
Partner, StoneTurn
ltenery@stoneturn.com
+1 312 775 1210

Ross M. Rustici
Managing Director, StoneTurn
rrustici@stoneturn.com
+1 617 570 3716

The world in which multinational organizations operate today is fraught with complex and ever-evolving risks. However, just as an effective General Counsel and/or Chief Compliance Officer enables the business to seize opportunities while staying within the bounds of acceptable risk — a robust security program can reduce, shape, and mitigate the nature of threats but should not be expected to eliminate threats altogether, particularly cyber threats.

As SolarWinds correctly pointed out in its motion to dismiss litigation against its CEO and CISO (Chief Information Security Officer) resulting from a 2020 security breach: "Subjecting cyberattack victims, who never promised invulnerability to such crimes, to class action securities fraud claims would undermine the... intent and fuel securities litigation in the wake of every cyberattack."

Cybersecurity, just like physical security and compliance programs, is about *managing* **business risk**. By definition then, a well-designed and implemented program is created with the expectation of some losses. Determining an organization's specific risk appetite with regard to cybersecurity requires a close partnership between security and business leadership. Too often however, CISOs are unable to answer the below questions, which may explain why the average tenure of a CISO is just 18-24 months:

1. What is the primary way which my company makes money?
2. What are the core value propositions of the company's services or goods?
3. What key assets are required to deliver those core value propositions?
4. Where is the business attempting to expand, change, or adapt its core offering?
5. What technology and programmatic elements will be required to enable those plans?

The C-Suite can enable better risk management by socializing security professionals with the rest of the organization and supporting their understanding and appreciation of operations. Successful CISOs understand their company's business and are able to align the security program to **enable** business imperatives and enhance shareholder value. After all, a CISO must fundamentally understand the business they are entrusted with protecting in order to create a defensible plan to enhance security while combating excessive business risk.

What a Successful CISO Should Consider

The foundation of any successful security program is understanding what you are trying to protect. Once the CISO understands the business, the drivers, and the goals, they can then create a smart plan to reduce risk based on asset criticality.

Asset criticality is more than just the "crown jewels" or even the latest buzzword of Zero Trust. It is about understanding how the business operates and how to protect the critical processes, which sometimes involve (but rarely starts and ends with) data. Once you understand the *what*, then you can start formulating the *how*.

While security fundamentals are a requirement, they do not always provide significant reduction in risk: Organizations must patch, implement asset tracking, standardize configurations, and deploy technology that is required by regulation or law. But these tactics are called fundamentals for a reason; these controls and measures are designed to create a base of security akin to installing a dead bolt on a glass door. Does it increase the level of effort required to break in? Yes. Does it add any significant impediment? No.

Once the fundamentals are implemented, the tailoring of security controls to business risk is what will make or break the security program. Think about your network in terms of the contours of the battlefield; IT security professionals should work to create impediments and areas of natural flow. The goal of implementation should be twofold:

1. Harden the key business processes/assets to the fullest extent possible
2. Understand and channel intrusions to more dispensable areas of the network

It is very rare that an intrusion uses only zero-day exploits for the full exploitation of a network. Building defenses around the assumption that even with the most hygienic regime, zero-days or human error could undermine the hardened perimeter, allows you to channel the adversary by creating paths of lesser resistance to areas where the security program can engage directly without impacting the core business.

Successful implementation has more to do with knowledge, planning, and exercises than

technology. At this point, a program can build a highly functional security stack with almost all opensource tools. The technology spend should not be the focus of the plan or the justification; rather, the CISO must be able to explain how their actions are creating barriers to disruption from malicious activity around key resources and how the overall posture is reducing current-state risk to business operations. This reduction in risk enables the business to become more aggressive in planning and projections because the CISO, like their GC and CCO counterparts, can help resolve impediments to revenue and earnings growth.

How the C-Suite Can Support

The Security department is often in a uniquely disadvantaged position. They are frequently:

- isolated from the day to day of the revenue centers;
- raised in a technology environment that provides little background or understanding of business operations;
- have terribly designed Key Performance Indicators (KPIs), and
- challenged with quantifying security risks that are inherently difficult meaningly metric.

The first two points can be remedied by cross-pollinating the security team with the revenue centers. By providing insight into, for example, how and why Engineering teams spin up shadow infrastructure due to their own pressures and deliverables, it is possible for Security to work with Engineering to provide a flexible and more secure solution. This understanding will also reduce policy controls and other rigid security regimes that result in such poor adherence that they might as well not be codified at all.

The third point is far harder. How does one create metrics and KPIs where success is a negative outcome? The drive for data and metrics often results in presentations from the security organization that have no legitimate meaning other than to provide numbers. What does it mean to have 10,000 validated alerts in a quarter? Is that a lot, is it a little? Does a change over time represent an improvement from a program perspective or just a change in terms of threat? No one can answer those questions with any level of certainty, making such indicators pointless. As the security program focuses on business enablement, their KPIs should be shaped in a similar fashion. Much like infrastructure teams are judged on system uptime, security teams should have similar metrics: how many cyber incidents resulted in business impact? Of the business impact created how much was to critical business systems and how much was to low-value areas of the network? Posing the metrics in this way helps put the business value of security into perspective. It is not about absolute wins and losses, but rather how well the core value was protected in a volatile environment.

Finally, organizations often have significant difficulty in quantifying the possible losses associated with cybersecurity incidents. Direct costs generally encompass technology down time, overtime, external support for incident response, and outside counsel, as well as potential monetary losses resulting from direct theft or regulatory fines. Indirect costs can include negative impacts to PR, marketing, customer

retention initiatives, and stock price. As covered above, an organization must pursue a strategy which involves trade-offs and risk acceptance in a way that still enables the business to achieve its mission and create value for stakeholders. Increasingly, savvy CISOs and security stakeholders collaborate to align the organization's risk management approach with the financials and the culture of the organization while also leveraging residual risk management tools like insurance. Practically speaking, and to attempt at least general quantifications, security leaders should consider evaluating threat models and hypothetical incident situations that realistically simulate impacts and losses to critical assets. The modeling should also include general estimations of possible losses contrasted with the impacts of cost-effectiveness estimates to realistically consider how approachable security investments might be to attempt to treat or accept a particular set of risks.

Conclusion

By orienting security programs to coalesce around business risk and enablement rather than absolute security, companies will become more effective in their operations. Security programs should not be viewed as loss centers but instead as essential parts of the organization to enable business operations. CISOs should provide guidance on how to best seize the next opportunity, while security teams can help manage and mitigate risk to enable those additional business opportunities.

Increasingly, businesses are operating in a world where consumers and partners often develop their first impressions of your organization from online and virtual interactions. Bringing in the security team earlier in the planning process allows for smarter architecture, smaller capital expenditures, and less overall risk.

Prevention is always more cost effective than remediation in the long run.

About the Authors

Luke Tenery, a Partner with StoneTurn, brings nearly 20 years of experience helping leading organizations mitigate complex cybersecurity, data privacy and data protection risks.

Ross Rustici, a Managing Director with StoneTurn, has over a decade of experience advising governments and global corporations on cybersecurity matters, as well as building security and intelligence programs for clients.