ISSN: 2755-0214

Journal of Economics & Management Research

Review Article

Open Access

How Can a Business Ensure Seamless Operations in Security, Breaking through Siloed Operations, Friction to Fusion Mindset

Pranith Shetty

Information Security & Risk Lead, Cisco, New Jersey, United States of America

ABSTRACT

There is a need for a dedicated security team in businesses especially due to the evolved Cybersecurity threat landscape, the techniques and attacks have become more sophisticated than ever. There are numerous variants of basic cybersecurity threat like social engineering. The scope and reality of lateral attacks is now more than ever. Dedicated and spanned security teams work with a singular vision of ensuring minimal to no business impact due to security risks, however this vision takes a hit if the operations amongst teams are siloed. Executives & management especially CISOs need to have access to centralized repository of data that brings in data from all security teams and not just one or two. Lack of collaboration and separate charter amongst security teams significantly impact the business decisions thereafter, there are various factors contributing to this effect. The article here firstly introduces the basic rationale of these instances occurring and then gets into the context, foundation on the teams involved, eventually describing the method that will help alleviate these concerns and risks.

This article is meant to articulate a solution that has worked in a few firms and can be easily replicated across industries, in solving the problem of siloed operations not only in security but also between security and engineering teams.

***Corresponding author**
Pranith Shetty, Information Security & Risk Lead, Cisco, New Jersey, United States of America.

Received: August 10, 2022; **Accepted:** August 17, 2022; **Published:** August 24, 2022

Keywords: Siloed Security, Siloed Operations, Friction between Teams, Cybersecurity, Risk Management

Introduction

As the cybersecurity threat landscape continues to intensify, it's surprising to see most companies still marching forward with the belief that security belongs exclusively in the hands of chief information security officers (CISOs). The mindset needs to change since CISOs alone are not responsible, they are more in executive capacity to streamline the security operations and ensure the betterment of risk posture within the organization, it's a shared responsibility between management and security teams [1].

Companies need to take a step back and think about security risks holistically, for example any incident is not the problem of incident management alone. There are set of stakeholders who need to be involved as per the incident management procedures. Everybody has a stake in it.

Threats from cyberattacks increase day by day due to the ever changing risk landscape, new techniques and attack vectors adopted by attackers, however in the presence of friction between IT and security teams, these attacks could very much be successful [2].

Any business or organization is divided into various teams based on their skillsets, requirements of the organization, business vision and objectives.

Conflicting goals and priorities are also one of the key reasons, for example creating products and getting them to market is one of the key goals for engineering teams but security teams are more concerned about secure products which delay the "get to market" timeline and this results in conflicts between teams, which ends up creating more challenges for the overall business [2].

It's not that security is not important but its de-prioritized in most cases.

Security should also be seen as a "department of yes" instead of no by Engineering teams, this is mainly is the result of security teams not acting as an enabler from the inside meaning working with the engineering teams but sitting on the sidelines and getting involved only on a need basis, the fault here is on both sides, engineering teams for not involving security teams during the design and development phase, as a result, it's too late to provide security recommendations and on the Security side for not recommending solutions but only listing problem or findings.

While there are challenges in bringing diverse teams together, it's not impossible, with proper strategies and alignments, teams can come together to work on a singular vision, communication between teams is key, a mediator team such as the Risk management teams can help bridge gaps between various teams and act as an intermediary for communicating successes and failures of the security teams to leadership, the drawback mostly is Risk management teams are not utilized to their fullest extent, collaboration is a two way street where the risk management teams often try to co-ordinate but fail to get timely responses.

Literature Review

This article here from a cybersecurity consulting firm, explains why Siloed teams are not helpful and significantly impact the operations of an industry especially Financial Tech. There are advanced attack campaigns targeted towards siloed security functions as per this article here from a cybersecurity magazine, Disparate charters, collection of tools does create a gap in security operations thereby opening the firm to cyber-attacks, this eventually beats the purpose of having a dedicated security team, these articles from independent consulting firms and magazines listed in this paper shed some light on the shortcomings and consequences of having siloed operations [3].

Various Roles in Security and their Functions

Every organization is set up to achieve a unified business goal, in this age of cybersecurity threats, it's very important to have a dedicated security arm with various teams that help defend the firm against threats and the ever evolving landscape. with a little proactivity and cross team communications, you can help all teams involved [4].

There are Mainly Following Teams Involved in Security Related Efforts

- **Application Security or Product Security:** This team runs point in ensuring the productor application being deployed is secure from all fronts meaning the architecture makes sense, there is no case of open ports or hardcoded procedures/functions with credentials. They are also responsible for offensive security related efforts meaning either performing penetration testing themselves or contracting it to 3rd parties for black box, gray box sort of testing processes. This team would also be involved in identifying vulnerabilities and working with Product teams in remediating those identified gaps.
- **Security Operations:** This team is the backbone of defensive security measures since it handles the key areas of Vulnerability management and Incident management. Vulnerability management team constantly is on the lookout for vulnerabilities from scans, or external reports. Incident management is on the line of fire with respect to incidents, based on the criticality of the incidents, the team is under pressure to contain, remediate and engage stakeholders within defined SLAs (Service Level agreements)
- **Governance and Risk Management:** This team is the one that can quarterback the whole security and risk portfolio, to ensure collaboration between various teams like product security and security operations mentioned above, Monitor and track these risks identified towards completion, prioritize based on business vision and goals. Communicate these via risk reports to the leadership and senior management. The risk management team can also work with the central policies team to ensure the security and engineering teams are working within the boundaries of the policies and procedures defined.
- **Project Management:** The PMO office is usually the team that hosts the steering committee conversations, they run point on some of the bigger and strategic projects, they keep track on the overall activity of the various security teams, reporting to the CISO or similar executive.

The following is a basic example of what a Red team that is Offensive Security's priorities are, what's some of their key objectives, while in Blue is Defensive Security team that is more on the reactive side of security trying to constantly monitor and handle risks. While in Purple the overall are teams like Governance and Risk management that work with both teams trying to understand the risk posture, identify and communicate risks to management, ensure there is appropriate risk response based on risk appetite and organization context [5,6].

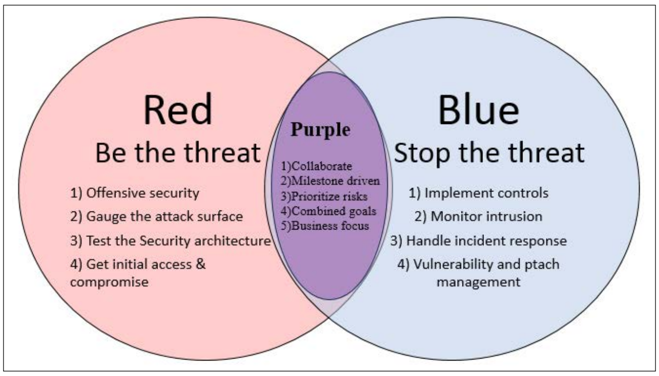


Figure 1: Red Team vs Blue Team

Risk and Compliance

Regulations are getting more and more stringent ensuring heightened visibility around corporate governance and practices. Noncompliance to regulations give way to heavy fines and sanctions which has a direct significant impact on the business. These events not just impact the business financially but there is a repercussion in the form of reputational impact [7].

Compliance and Risk management both are key functions to avoid these risks.

Compliance: Activities that a firm or organization have to adhere to, could be set of internal policies or external regulations.

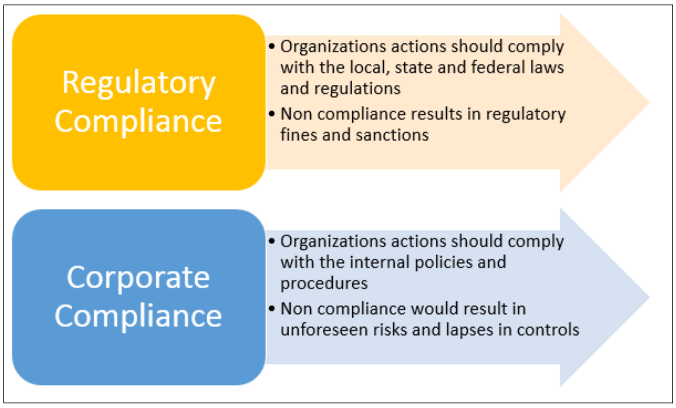

Regulatory Compliance
• Organizations actions should comply with the local, state and federal laws and regulations
• Non compliance results in regulatory fines and sanctions
Corporate Compliance
• Organizations actions should comply with the internal policies and procedures
• Non compliance would result in unforeseen risks and lapses in controls

Figure 2: Regulatory Compliance vs Corporate Compliance

Risk Management: Risk Management is the process of identifying, assessing, and managing potential threats that could damage the organization's ability to achieve its business objectives.

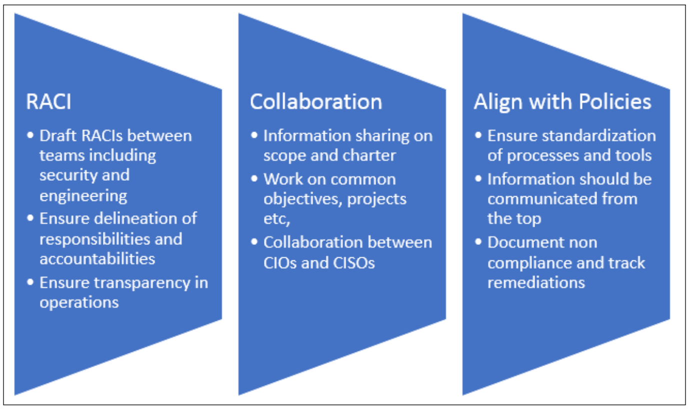
The key steps involved in this process include understanding the organization's context, identifying risks across the business through various channels, analyzing them, risk rating those risks, communicating with management to figure out the appropriate risk response, finally reporting these risks periodically to ensure these are monitored and tracked towards remediation.

Method & Use Cases

The idea that only management is responsible for ensuring there are no siloed operations within their teams is not an accurate statement, the message needs to come from management, yes! However, staff members are equally responsible to ensure there is transparency and information sharing between teams.

There are few tried and tested techniques that help break down siloes within security teams, RACIs between teams ensure there is proper delineation between teams charter and ensure there is no one stepping into others shoes.

Teams should invite each other to work on projects that share a common goal, diverse skillset as within teams help achieve objectives quicker, more collaboration will lead to increased bandwidth amongst resources and everyone will be able to work on a collective vision [8-11].


RACI
• Draft RACIs between teams including security and engineering
• Ensure delineation of responsibilities and accountabilities
• Ensure transparency in operations
Collaboration
• Information sharing on scope and charter
• Work on common objectives, projects etc,
• Collaboration between CIOs and CISOs
Align with Policies
• Ensure standardization of processes and tools
• Information should be communicated from the top
• Document non compliance and track remediations

Management should treat everyone with empathy, try to understand the ground reality and operations so that they are more connected on the tasks, this will help management strategize solutions that are practically feasible.

Security teams while working with engineering should work in advisory capacity since accountable teams are product and design, Security teams are consulting them on security controls and measures, they are not responsible and accountable for creating products.

There should be alignment across teams in terms of policies and procedures so that staff within the organization follows the same set of prescribed policies and procedures.

Teams like Governance and Risk management can step in and try to collaborate with all teams in security at least from a security and risk standpoint, drawing out RACIs, this team can align their charter with the Project Management Office (PMO) to ensure right visibility and oversight to the CISO and leadership up the chain.

Conclusion

All teams within the business, are created with a specific collective vision but post creation they eventually end up having their own mode of operations, charter and agenda.

This is a result of lack of information communicated between management and teams within. Lack of trust, transparency and collaboration also results in division in operations. Some security teams are used to function with a comprehensive set of tools, however, it's not feasible across all teams. There has to be a predefined and agreed method for integration devised. Lack of transparency also results in unclear charters between teams, management support and direction play a crucial role in ensuring teams under their command are constantly working towards a unified vision. Moving goal posts don't help or contribute to this effort so it's important to have a stable set of vision and objectives at least for a fiscal year. This ensures clarity in message communicated, and once teams collaborated using the methods listed in the afore mentioned sections, siloed operations would cease to exist.

References

1. Albert D (2020) Council Post: Why Security Can't Live In A Silo. Forbes. Available: https://www.forbes.com/sites/forbestechcouncil/2020/10/05/why-security-cant-live-in-a-silo/?sh=4a7ccbe33819.
2. Netscout (2022) 5 Steps for Improving Collaboration Between IT and Security Teams. CSO. Available: https://www.csoonline.com/article/571933/5-steps-for-improving-collaboration-between-it-and-security-teams.html.
3. Smith T (2022) Cybersecurity: Why Siloed Teams Are Killing Fintech Defences. The Fintech Times. https://thefintechtimes.com/cybersecurity-why-siloed-teams-are-killing-fintech-defences/
4. IANS Faculty (2022) Understand the Roles of Red, Blue and Purple Teams, IANS. https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/04/19/understand-the-roles-of-red-blue-and-purple-teams.
5. RiskOptics (2022) Compliance vs. Risk: Similarities + Key Differences. Available: https://reciprocity.com/blog/compliance-vs-risk-similarities-key-differences/.
6. NIST (2022) risk management - Glossary | CSRC, csrc.nist.gov. https://csrc.nist.gov/glossary/term/risk_management.
7. Rutrell Yasin (2016) How Security And IT Teams Can Get Along: 4 Ways. Available: https://www.darkreading.com/cybersecurity-careers/how-security-and-it-teams-can-get-along-4-ways
8. Will Kelly (2021) 6 tips for better collaboration between security and cloud teams, CSO . Available: https://www.csoonline.com/article/570635/6-tips-for-collaboration-between-security-and-cloud-teams.html
9. GuidePoint Security (2021) Closing the siloed security gap with cybersecurity program management. Available:https://www.guidepointsecurity.com/blog/closing-the-siloed-security-gap-with-cybersecurity-program-management/.
10. Chesla A (2016) Why Advanced Attack Campaigns Like Security Silos. Available: https://www.securityweek.com/why-advanced-attack-campaigns-security-silos/.
11. NIST (2022) Risk Appetite - Glossary | CSRC. Available: https://csrc.nist.gov/glossary/term/Risk_Appetite.