MANDIANT

WHITE PAPER

# Rationalization

# Cyber Security Rationalization: Aligning IT and Finance on Organizational Risk

A company's most important assets include not only its data, but its reputation and trust with customers and investors. Without them, transactions fail to flow and valuations can plummet in public and private markets. The cyber security technology, teams and policies that protect that reputation and trust are no longer unknown quantities in the marketplace for non-IT experts.

Customers and investors alike are pricing it into their valuations of business relationships and corporate economic health. This undeniable connection between a firm's cyber security and financial health has garnered the attention of board members who now see cyber security as an important part of their fiduciary responsibility. Add to this the current challenges of an increasingly risk-sensitive and pandemic-aware world, and the mandate becomes clear that CISOs and CFOs must work together in new ways. How they attach real metrics and proof behind their answers to the age-old question "Are we safe from attacks?" may well determine the financial future of their company.

Every business' risk tolerance for attacks and its cyber security environment are unique and constantly changing in response to actions and expectations in the marketplace. There is no one size fits all set of security tools to set and forget under these circumstances. Cyber security leaders need to know how effectively they are detecting, alerting and blocking threats in relationship to the level of risk they are willing to accept against prioritized types of attacks—every minute of every day. And their partners in the office of the CFO need to clearly see the connection between the acceptable risk level that the company sets, the effectiveness of the CISO's security measures and the financial rationalization of the tools and people required to deliver a specific level of security and protect the value of the company.

### Cyber Security Spending is Out of Control

The average organization uses 30-70 security tools and sometimes spends millions of dollars to address a single type of attack. According to the **Cybersecurity Market Report**[1], worldwide spending on cyber security is predicted to top $1 trillion by 2022. While more than 500 cyber security companies in the market today may profit, their customers may not be any more secure.

Not only has the level of spending increased and outpaced the losses the technologies are designed to protect, but cyber security has gained a reputation as a black hole within corporate walls. Money is spent without demanding verification of effectiveness.  Accepted practice has been to answer the question of "How much do you need?" with "As much as I need to protect from threats." This response must change to a quantitative valuation of effectiveness and rationalization that can only be achieved by continuous stress testing that accounts for corporate risk profiles with financial implications in the marketplace. Cyber attacks have an impact on reputation, trust and stock price—and costs of recovery often exceed insurance coverage. Cyber security has become an expensive part of an organization that must be held accountable in new ways and be the subject of new kinds of conversations.

Cyber attacks have an impact on reputation, trust and stock price—and costs of recovery often exceed insurance coverage

[1] Cybersecurity Ventures' 2019 Cybersecurity Market, June 2019

# New Cyber Security Conversations

In 2019, before the full impact of the Covid-19 pandemic, changes were already underway in the conversations between company CISOs and CFOs. These conversations resulted from the intersection of three trends in cyber security: growth in spending, board questions and pressures, and shortcomings in cyber insurance policies.

### 1. Exponential Growth in Cyber Security Spending Within IT Departments

The large expenditure for cyber security no longer went unnoticed. The common feeling was that spending was out of control, and far outstripped the effectiveness the technology provided against risk priorities. But companies did not have hard evidence to support their supposition.

### 2. Board Questions and Pressures Around Cyber Security Effectiveness and Compliance

As fiduciaries, the board increasingly faced both legal and financial ramifications of breaches. These costs were not only passed on to customers, but also manifested in hits to the financial valuation of the company in public markets. Boards began to ask new kinds of questions that demanded increasing levels of education and insight into a company's cyber security and its effectiveness. They began to see IT and cyber security expenditures and effectiveness as part of their fiduciary responsibility, just like all other operational areas.

### 3. Shortcomings in Cyber Insurance Policies

Cyber insurance was about as well understood as cyber security IT purchases. Very few people knew how it should be priced, while policy scrutiny was on the rise. Companies did not want the exposure of being under-insured, but recovering from an attack often exceeded their insurance coverage. Many acts commonly understood among technology professionals to be cybercrime – such as ransomware – were not deemed as criminal acts by the insurance industry.

As a result of these trends, CISOs began to place a higher priority on integrated platforms for their cyber security IT stack, rather than the often duplicative and rarely optimized point solutions that they had purchased in the past. They sought out visibility into how effectively security controls (such as email, endpoint, network and cloud controls) actually performed against various attacks and risk scenarios. Conversations about this information with CFOs evolved the analysis to rationalization, which involved financial justification for security spending on tools and people being mapped against agreed upon risk profiles. The hope was to achieve more effective protection against the risk prioritized areas of the company at a lower level of spending.

# Cyber Security in a Pandemic-Affected World

The 2019-2020 global pandemic has increased stress on companies and their IT teams with the dramatic growth of work from home environments, and as video conferences and streaming become essential lifelines to human connection and entertainment.  Cyber security teams have scrambled to change and scale technology, processes and policies to enable the secure and reliable use of home systems, networks and endpoints that were never intended for business use.

## Crisis Readiness

Crisis readiness and responsiveness now top the list for cyber security priorities in most companies. With the impact of the COVID-19 pandemic, data analysis policies are forced to prepare for new kinds of security exposure as highly secure business information now travels regularly into home devices and networks. Security readiness for 24-7 remote usage and home network security differs significantly from that within the corporate firewall. Security teams are now challenged to deliver full corporate security in this environment while justifying the ROI of their spend. This significantly impacts IT, as more companies discuss permanent or more widespread work from home options post-pandemic. The very nature of work is changing and cyber security must respond in real time.

### - Falling Profitability

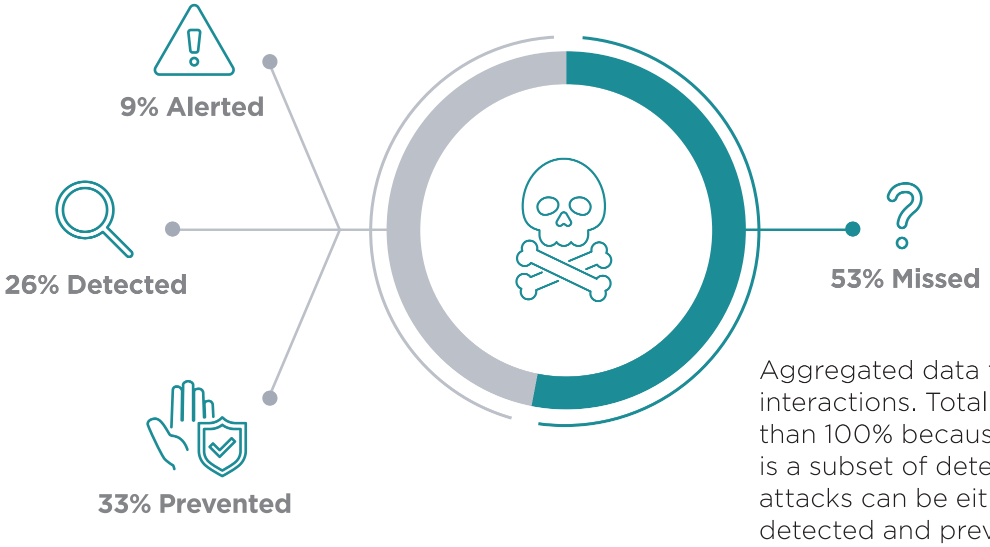
With a few unusual exceptions, most companies and industries are enduring massive hits to their bottom lines. Even with new demands for cyber security measures to protect work from home, falling profits place pressure on the prioritization of efforts and rationalization of expenditures for technology and staff. Security weaknesses were not always understood pre-pandemic and they are even less clear now. Budget decisions need to be based on more than a simple tradeoff between the costs of technology and people. With smaller amounts of capital available, tough choices around the ranking of specific security priorities will need to be made, while parallel financial pressure exists for maintaining or even decreasing security risk levels.

### - Increased Financial Scrutiny

As the structural essence of many industries is challenged, no area of business—not even IT—is safe from scrutiny. Demands for financial justifications for IT expenditures at companies are now much higher more likely than before the pandemic. So far in 2020, IT budgets are flat or significantly falling. Cyber security companies receive requests from long-time customers for significant discounts on current technology products. ROI is becoming as much a watchword for the CISO as it has always been for the CFO.

### - Changes to Infrastructure Requirements

During the pandemic, strategies for financial sustainment of the business are being prioritized, with focus on rebuilding infrastructure and reducing risk in 2021 and 2022. Sustainment focuses on clearly determining the digital assets that must be protected along with those assets for which security can be removed or minimized for the moment—given an overall corporate risk profile revised in light of COVID-19. The financial ROI of cyber security technology, policies, and people against that risk profile is the new metric, with rationalization at the forefront of the CISO-CFO-board dialogue. And that will continue to be the case in the post-pandemic world as well.



Aggregated data for attack interactions. Total is greater than 100% because alerted is a subset of detected and attacks can be either or both detected and prevented.

## Rationalization – People, Policy and Technology

Companies need to look at their cyber security spend through the lenses of both effectiveness and rationalization.

Measuring security effectiveness essentially means validating how well security controls perform to their expected outcomes – and doing so on a consistent, ongoing basis. The challenges and complexities of having unique environments, multiple teams and constant change require that security programs evolve continuously. CISOs and their teams need to continuously measure and monitor controls to capture quantitative evidence of security gaps so they can demonstrate with evidence the ability to reduce risk and improve the organization's overall security posture. This allows them to prove effectiveness.

After **validating effectiveness** against prioritized security use cases and the company risk profile, the next step is **rationalization**—the attachment of financial value to that level of effectiveness.

Rationalization, a relatively new cyber security concept, has emerged as a result of increasing pressure from boards and the C-suite. They are demanding that collaborative teams of CISOs and CFOs provide hard data around both the effectiveness and ROI of their cyber security spend against prioritized attack types and the company's overall risk profile. They also want to verify a company's ability to recoup its cyber security investment, which involves articulating and measuring value lost in successful attacks and relating that to the ability to improve effectiveness through the use of cyber security technology.

Rationalization must be a continuous process focused on aligning a company's cyber security arsenal—technology, people and policy—with desired security and risk levels as well as financial and corporate value outcomes.

### Technology

What is the **data-validated ROI** of the cyber security spend needed to deliver specified security effectiveness levels given the risk profile of the company? What is the financial implication of the manner in which security outcomes map against priorities and costs? Within specific attack types, how are product overlaps identified and eliminated so that costs can be cut or dollars reallocated to more important areas?

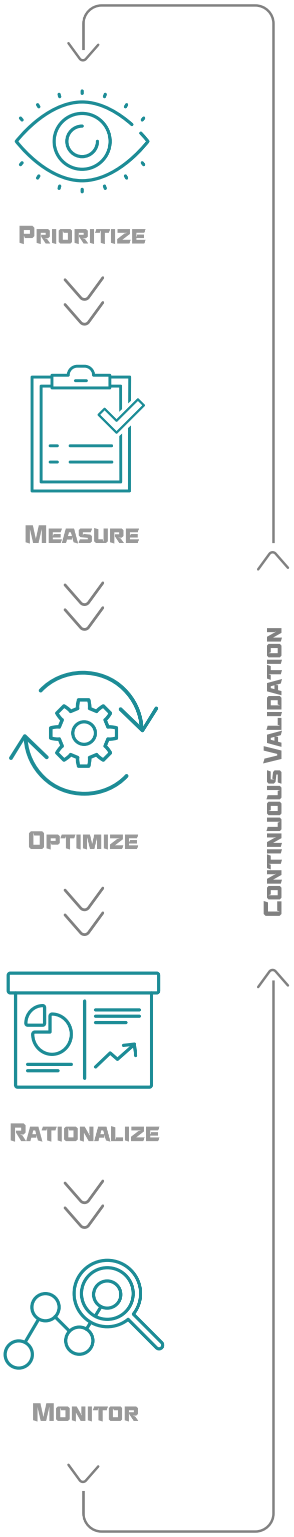
### People

Is the company **investing** in skill development to acquire the competency levels needed to protect the security environment? Have duplicative technology solutions been eliminated in the technology stack so teams are not spending time attempting to optimize unnecessary tools and platforms?

### Policy

How do new policies reflect the company's overall **risk profile** and risk tolerance against specific attack types? How do policies directly impact the company's **value** in the marketplace?

Rationalization is meant to help organizations see what they need to do to get as close as possible to obtaining the maximum value from their investments. This goes beyond the old technology discussion of: "Are we going to get hacked or not?"



# The Five-Step Framework of Mandiant Security Validation

Mandiant experts use a five-step framework to continuously measure a company's security effectiveness, validate security performance and financially rationalize cyber security investments. All of this is set against a company's consciously constructed risk profile. At the core of this framework is the mandate to value actual quantifiable evidence of performance over qualitative handwaving and assumptions of the past.

This framework is not about action at a single point in time. It is about establishing an environment of continuous vigilance and validation in response to the acts of hackers, IT infrastructure drift and unforeseen acts of nature.

## 1. PRIORITIZE

**Questions:**

- What threats are most likely to target our organization?
- How prepared are we to address those threats?
- What behaviors are our adversaries using to breach other companies?
- How should we prioritize resources?
- How do security technology, programs and resources align against the most likely threats and actors?

**Actions:**

- Proactively identify threats
- Use real-world adversary tactics, techniques, and procedures rather than simulations
- Use comprehensive threat coverage with an equal focus on both technical attacks and adversary tactics across multiple attack vectors

## 2. MEASURE

**Questions:**

- How can the relevance of threat intelligence and exposure to a likely attack be measured?
- How can an accurate quantified baseline of the effectiveness of a company's current cyber security level be set, given the existing technology stack, policies and people?
- How will you gather qualitative evidence to demonstrate effectiveness?
- How will you use the qualitative evidence of controls behavior and performance to drive improvement?
- How will you accurately assess security infrastructure health?

**Actions:**

- Gather qualitative evidence of effectiveness
- Use precise knowledge to drive improvement
- Assess security infrastructure health

## 3. OPTIMIZE

**Questions:**

- After clearly identifying gaps and shortcomings, or in response to corporate changes in a business' risk profile, how can effectiveness be maintained or increased?
- Now that you have specific controls-based visibility, where will you pinpoint improvements across people, processes, and technology?
- How will you shift to proactive testing with real, full lifecycle attacks?

**Actions:**

- Gain specific controls-based visibility
- Improve effectiveness of security tools
- Shift to proactive testing with real, full lifecycle attacks

## 4. RATIONALIZE

**Questions:**

- How can a financial value be attached to cyber security effectiveness?
- How can financial and resource spend be justified, reduced and optimized (through elimination of duplication and waste), while simultaneously maintaining or increasing security effectiveness in areas such as executive communications, remote working protocols and customer data protection?
- How can financial rationalization demonstrate alignment between the efforts of the cyber security technology stack, policies and people with the desired outcomes, priorities, costs and risk profile of the company?

**Actions:**

- Leverage definitive proof of control performance
- Measure impact values to security posture
- Apply quantitative data to ROI analysis

This framework is not about action at a single point in time. It is about establishing an environment of continuous vigilance and validation.

## 5. MONITOR

**Questions:**

- Knowing that both the overall cyber security environment and a company's risk profile are not static, how can effectiveness and performance be monitored to inform proactive response?
- Can you maintain confidence with operational effectiveness?
- There will always be changes in the environment; how will you avoid deviations in performance?
- How will you inform the business with automated monitoring and reporting?

**Actions:**

- Maintain confidence with operational effectiveness
- Avoid deviations in performance
- Inform with automated monitoring and reporting

# The Need for Rigorous Cyber Security Rationalization

It used to be acceptable for cyber security measures and risk metrics to be anecdotal and concentrate on perceived risk mitigation. But increased cyber security budgets accompanied by declining effectiveness against ever-increasing attacks brought this practice into question. The added pressures of the COVID-19 pandemic, resulting in falling profitability and rising work-from-home security concerns, have made qualitative answers less relevant than quantitative answers when it comes to technical effectiveness and financial rationalization of security spend. Corporate mandates now exist to specifically measure, optimize, validate and monitor the effectiveness of technology, people and policies against the risk profile of the company and prioritized attack types. Operations must be sustained under difficult circumstances, costs must be cut, duplicated efforts eliminated and corporate value maximized in the public markets.

Cyber security now requires a company's CISO and CFO to work together to answer the fiduciary questions of a more educated board and financial markets that revolve around the specific measurable value (budgets and stock price) that comes with effective security rationalization.

Operations must be sustained under difficult circumstances, costs must be cut, duplicated efforts eliminated and corporate value maximized in the public markets.

Know the true measure of your cyber security on a daily basis, visit: **www.FireEye.com/mandiant/security-validation.html**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

**About Mandiant Solutions**

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.