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.

Cyber Security Rationalization: A CFO Discussion
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 attacks have an impact on reputation, trust and stock price—and costs of recovery often exceed insurance coverage.

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 Report¹, 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.

¹ Cybersecurity Ventures’ 2019 Cybersecurity Market, June 2019
The Evolving Role of the CFO

The CFO is responsible for the financial efficiency and accuracy of a company. If financial systems are compromised through a cyber attack, the reliability of financial reporting comes into question, which, in turn, can directly impact a company’s performance and value in the public marketplace. Without the ability to demonstrate competence in protecting this information, organizations face a dissipation of trust and suffer the consequences of revenue loss from customers and market valuation decline from investors—particularly as both groups (and the SEC) become more informed about the impact of breaches.

There are three main areas of questions that the CFO must be prepared to address—with tested data and evidence.

1. What is the ROI of our cyber security stack based on the agreed upon corporate risk profile? How is this demonstrated?
2. How are we recouping our cyber security investment overall, as well as within prioritized application categories?
3. How does the company cyber security scorecard compare to the financial rationalization of security spend?
New Demands from the Board

Investors and regulators are placing increased pressure on companies to articulate and provide specific proof about how they invest in and use cyber security technology to protect the digital assets, executive communications and value of the company. At the same time, the board is asking why they need to care about cyber security and feeling uneasy about this new fiduciary burden in an unfamiliar area of the company.

Boards are asking for answers to questions such as:

1. Are we demonstrating and communicating due care and due diligence to customers and regulators in our cyber security efforts?
2. Is security performance in alignment with the company’s overall strategic direction or focus? How does it map to individual areas of security prioritization? Is effectiveness trending in the right direction?
3. How have the CISO and CFO lowered costs while also increasing security? Are there sufficient resources to continue to implement this level of cyber security? What if we need to lower costs again?
4. How do our efforts compare to those of our industry peers?

The board is asking why they need to care about cyber security and feeling uneasy about this new fiduciary burden in an unfamiliar area of the company.
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
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

This framework is not about action at a single point in time. It is about establishing an environment of continuous vigilance and validation.
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](http://www.FireEye.com/mandiant/security-validation.html)

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.