OPTIV

OPTIV'S SIX FORCES OF SECURITY STRATEGY

Internal and External Forces that Impact Security Strategy

Jason Clark,
Chief Strategy and Security Officer, Optiv

James Christiansen,
Vice President, Information Risk Management, Optiv

James Robinson,
Director, Risk and Threat Management, Optiv

Renee Guttmann,
Vice President, Information Risk, Optiv

Abstract: Through thousands of engagements with leading organizations, Optiv has identified six essential forces that come into play when building a secure environment. These forces, both internal and external, have significant impact on security strategy. Awareness and monitoring of these forces is essential to reducing risk, responding to change and anticipating threats. Optiv's Six Forces of Security Strategy can guide you as you consider the relative weighting of these forces and their influence on your security journey. CISOs should embrace Optiv's Six Forces of Security Strategy; and CIOs, CEOs and boards should ask their CISOs to do so if they haven't already.

Executive Summary

As a security leader, each and every day you use your limited resources to skillfully navigate a changing threat landscape and a myriad of organizational requirements. Charting a successful course means aligning operational excellence and security priorities, and meeting overarching business objectives. That requires people, processes and technology. But, it also requires a solid understanding of the strategic forces that impact your organization, and the ability to use that essential information to help you create a successful security strategy.

Through Optiv's work with thousands of clients, we've identified six main internal and external strategic forces that impact the security of every organization to varying degrees. We call them Optiv's Six Forces of Security Strategy:

1. Business Strategy
2. Information Technology (IT) Organization, Systems and Infrastructure
3. Organizational Culture
4. Adversaries and Threats
5. Government and Industry Regulations
6. Global Social and Political Forces

This white paper will help you understand Optiv's Six Forces of Security Strategy. It will provide you with the baseline information you need to assess the relevance and impact of each force on your organization. And, it will enable you to create a security strategy that more effectively manages risk, maximizes capital effectiveness, and empowers your organization to pursue business advantages.


Business Strategy
IT Organization, Systems and Infrastructure
Organizational Culture
Adversaries and Threats
Government and Industry Regulations
Global Social and Political Forces

Why Six Forces?

Today's most effective security leaders know how to couple tactics and strategy, and formulate a cohesive vision that is in-line with corporate culture and business objectives. However, the majority of security leaders are still assessing their program postures with some form of standardized risk assessment – looking at their organizations' controls and the maturity of their security services against standard frameworks.

Whether you're in the first or second category, you can significantly improve your organization's security success by addressing the main pressures, or forces, that drive a highly effective information security program strategy. Optiv has identified six of them. These are naturally occurring forces that impact every security organization regardless of size, complexity, industry sector or location.

Optiv's Six Forces of Security Strategy helps you better understand your environment, enabling you to implement strategic and tactical security measures as part of a security program approach. Considering these forces gives you the insight you need to make better and more business-aligned decisions regarding risk, budgetary spending and the assigning of critical resources.

Force 1: Business Strategy

Attempting to develop a security strategy without fully understanding the direction of the business is similar to navigating through a forest without a compass: You may eventually arrive somewhere, though likely not the desired destination, or even more likely, you will arrive with a number of unnecessary cuts and bruises. For this reason, understanding the business strategy of an organization is a necessary precondition of creating a highly effective security strategy.

Whether executives are focused on growing or streamlining the business, each carries complexities that are far different from one another. Here are three common business goals.

1. **Expansion through mergers and acquisition (M&A)** – when acquiring and/or integrating a company, you've got to apply as much scrutiny to your target's level of information security risk as you apply to all other aspects of their business. Some acquiring companies don't take this as seriously as they should, and end up buying security headaches. When working on a merger or acquisition, you need to carefully assess historic breaches; future threats; information security policies; and existing and future data – where it comes from, where it's held, how important it is, how it's segmented, who has access, and how it's protected. With M&A growth – both on the acquiring and acquired sides – some employees will invariably worry about their current positions and the future, which often leads to increased insider threat.
2. **Foreign expansion** – often means understanding the local economy, customs, regulatory requirements and threats. A security strategy that works well in the U.S. may be wholly inadequate in nation-states prone to spying or other forms of regionalized threats.
3. **Cost-cutting** – whether in the form of layoffs or "doing more with less," reductions in security budgets can lead to increased risk resulting from things like unpatched systems, lax system maintenance, and over-taxed staff, among other items.
4. **Organic growth** – increased competition to gain market share also increases insider threat, industrial espionage, and the need to provide customers with positive experiences. As a result, the necessity for transparent security practices also rises.

Small- to medium-sized businesses (SMBs) are not alone in overlooking strategy. The complexity of large enterprises often includes multiple business lines that have their own business strategy, culture, economics and markets. You must consider each of these business units when developing the overall security strategy, which requires flexibility in the security program to meet the individual needs of the business units.

Force 1: Business Strategy

To understand the impact of Business Strategy, ask:

- What is your organization's business strategy? How can your security strategy support that mission?
- What are your organization's most critical assets?
- Is your organization growing or consolidating?
- How resilient is your organization to an attack or incident that affects operations?
- Do you have a clear understanding of the business strategy?
- What is your go-to-market strategy?
- Do you have any M&A activity underway or planned?
- What drives the value in your company (customers, IP, brand, partners)?
- What are the critical assets that you need to protect for your business to sustain its market share and growth?
- Are you planning to move business operations to high risk countries?
- Is your business making changes that will increase the overall risk profile (e.g. reorganization, re-branding, etc.)?

Force 2: IT Organization, Systems and Infrastructure

The management and operation of a business's information technology systems, infrastructure and resources can have a significant impact on security strategy. From outsourcing business processes to the utilization of cloud computing to the influx of mobile devices within the corporate perimeter, the constantly evolving use of technology is affecting the way organizations approach security.

In order to develop an aligned security program you've got to understand the level and maturity of IT resources. A certain level of available resources is required to implement security technologies. And, understanding the maturity of your organization helps you determine how much diligence is needed to ensure that your IT environment is properly controlled and monitored. Maturity is also a key factor for many organizations when deciding whether or not to outsource parts of the information infrastructure, determining how to best manage an increasingly diverse device ecosystem, and responding to big data demands as well as other trends that dramatically change the way such infrastructure is managed and secured.

As more organizations embrace the various advances in technology, new services and delivery models, and other innovations, it's important to consider the differing impacts on security requirements. Here are some trends that are top of mind for our clients globally:

- Software-as-a-service (SaaS) requires a different security strategy than a full migration to an infrastructure-as-a-service (IaaS) cloud model.
- Bring your own device (BYOD) offers cost-shifting benefits, but has created new challenges for device management and security. Getting the balance right has proven difficult because organizations still have more work to do to ensure that the Internet of Things (IoT) doesn't introduce greater, unanticipated risks.
- Organizations struggle with data management policies, and that struggle is heightened with the push towards big data. As organizations increasingly create large, distributed data stores and work to derive insight through data analytics, these difficulties will continue to push security and business policies in new ways.
- Migrating IT security functions to managed service providers or the cloud can result in reduced costs and increased access to expertise on demand. Understanding the complexities of the security puzzle, however, is a challenge and many organizations fail to focus on a concerted due diligence effort to uncover hidden risks.

Managing information technology and IT security functions requires that your organization has a strategy to monitor internal and external business processes.

Force 2: IT Organization, Systems and Infrastructure

To understand the impact of IT Organization, Systems and Infrastructure, ask:

› Is a particular IT function a strategic asset to the business? If not, will you consider outsourcing it?

› What level of visibility and transparency does my company have into IT operations?

› To what degree are my company's business processes impacted by current IT trends such as BYOD, big data, IoT and the adoption of cloud computing paradigms?

› How strategic is IT to your business? Does your CIO have a seat at the table with your company's other senior executives?

› How much of IT is shadow IT or cloud (IaaS/SaaS)? How much of your IT is outsourced?

› What is the relationship between your CISO and IT? Does security report into IT or are they peers? Do they have a good working relationship? What are the lines of demarcation?

› Is your IT organization reactive or proactive?

› How mature is your IT organization?

All of your systems and services should be enterprise-ready and give you the level of transparency and granularity that you require. Any outsourced services should provide visibility into resource utilization and incident monitoring to help detect potential security incidents.

Aligning security strategy with IT management and functions allows you to ensure that your security organization and capabilities can support the enterprise's IT evolution from legacy internal infrastructure to the build, buy or outsource considerations of the future.

Force 3: Organizational Culture

An organization's culture can significantly contribute to the success or failure of its security program. The two must therefore be aligned. Understanding your executive team's appetite for taking risks and restricting the free flow of information, and gaining perspective into their view of how security should be perceived by the staff impacts overall strategy. There needs to be accountability for security across your organization from executives to individual contributors. If your organization is risk adverse then a more restrictive security strategy is appropriate.

The Impact of Corporate Culture Can Vary By Organization and By Vertical

Many hospitals have open cultures that allow them to quickly respond to emergency situations, but medical personnel are more interested in access than in data security. Injecting security into such an open-access model in the wrong way can be very difficult and potentially endanger lives. Cultures that require the free flow of information – such as hospitals, engineering companies, educational institutions and start-ups – need to adopt security strategies that allow more transparency while still reducing risks.

As a security leader, understanding organizational bias is critical to developing the right security strategy. You should interview and evangelize to your organization's top leadership. Does your organization aim for disruptive innovation or avoid market risks? How comfortable are your executives with technology? Technologically savvy executives – such as those at startups – will act as security enablers, while those managers who do not fully comprehend security may inhibit security efforts.

Similarly, other employees can be a security strength or weakness. Workers are often the first to notice an anomaly that could be indicative of a successful attack. However, users are also widely disparaged as the weak link in security. How your organization treats and empowers its users will have a tremendous impact on which security strategies are effective in your organization.

As a security leader, you should always be in tune with your organization's culture so that you can make sure that it aligns with your executives' view.

Force 3: Organizational Culture

To understand the impact of Organizational Culture, ask:

- Is your organization agile or static?
- Do executives support security or do you need to market to them?
- Are your employees receiving enough training in security processes and the importance of security?
- Is your culture creative, collegial and risk-taking or a hierarchical, process oriented, well-oiled machine?
- Is security everyone's job in the company? Do employees know the impact to your company if valued assets are compromised?
- How quickly does your organization accept change?
- Is your culture risk adverse or risk tolerant?
- Does your organizations' culture support alerting security if employees notice something suspicious?

Force 4: Adversaries and Threats

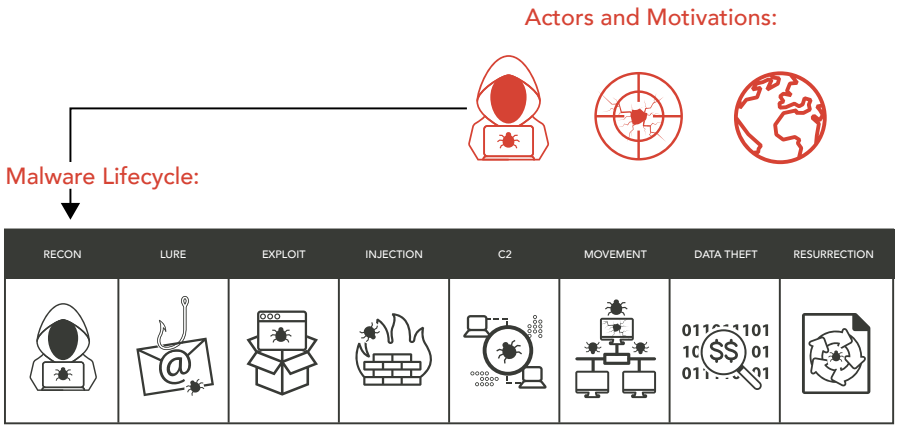
Threats faced by organizations vary greatly by industry sector and are advancing every day. A recent study indicates that about two-thirds of companies expect cyber threats to their business to worsen [1]. How do you effectively respond to these advancing threats? Shift your mindset: thinking like an attacker and understanding their process provides valuable perspective to help you harden your defenses and streamline your security investments. This technique is called threat modeling or kill chain analysis.

Threat Modeling

Picture your organization's most important assets, which may include customer credit card information, trade secrets or sensitive internal email. Protections such as firewalls are likely already in place, but are they enough? When a burglar tries to rob a house, they aren't deterred if the front door is locked. Similarly, once a hacker hits a firewall, they will simply find another way in. Threat actors use their own attack steps, which can be dissected and often anticipated by critically examining the ways in which the attacker may try to access your information. Figure out your top threat actor processes ahead of time, and your team may be able to prevent attacks by shutting down links in the attack process.

The threat modeling approach is widely recognized as prudent, however too few organizations use this method today. That's because many organizations are busy reacting to security issues, or need more resources to comprehensively test their systems against every potential threat. Shifting from setting up protection against attacks on all assets, towards using threat modeling to focus on the most important ones allows you to apply your understanding of common attack strategies and adversaries' tactics, techniques and procedures (TTPs). As a result, you can implement defense strategies that more readily maximize security return on investment (ROI).

Advanced Threat Lifecycle/Pattern



Force 4: Adversaries and Threats

To understand the impact of Adversaries and Threats, ask:

- What threats typically target your company's industry?
- Has your security team conducted an analysis to determine what the threats are?
- Are your organization's employees receiving enough training in security processes and the importance of security?
- What potential impact and risk do your third-party suppliers represent? Consider how to best mitigate those risks.
- Does your company worry about the insider threat?
- Do you know your threat actors? Who are your enemies? Who would profit from attacking your company?

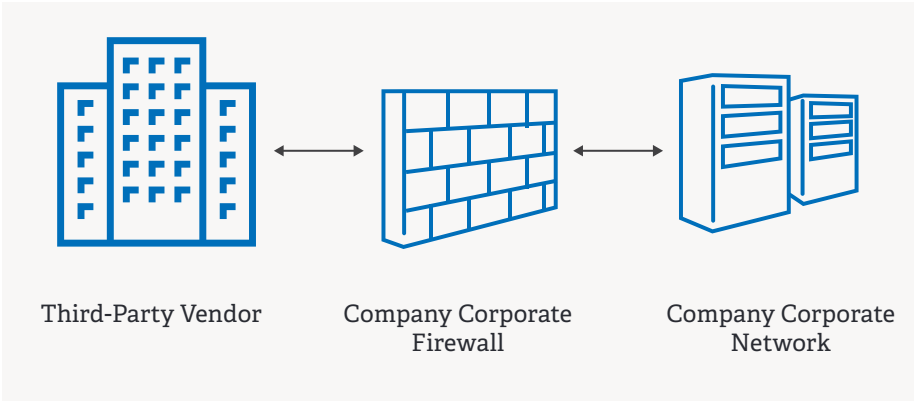
Organizations need a way to view the advanced threat kill chain and actors. Break down and understand these stages of the attack, and then ask what people, process and controls you have at each stage. In other words, what is the percent likelihood that your defenses will work, or the percent likelihood that the bad guys will make it to the next stage of the attack?

1 http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf

What about Third-Party Risk?

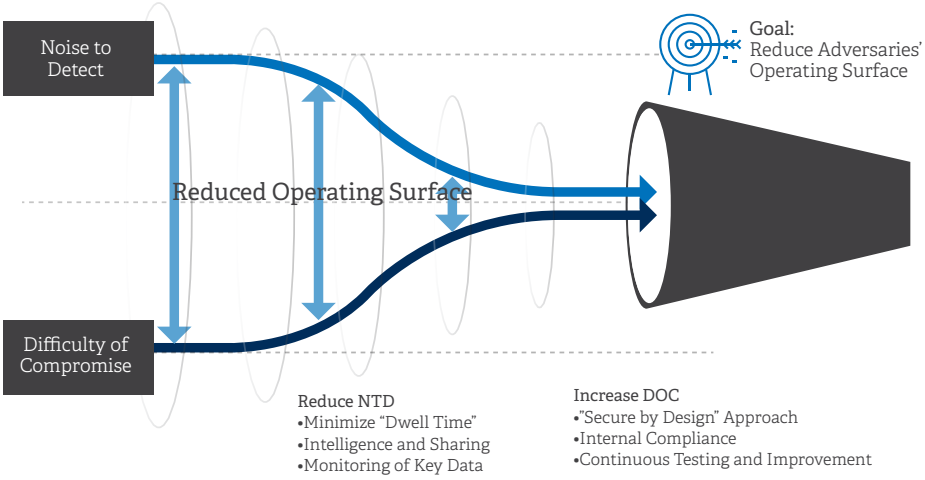
Many large companies allow third-party vendors to have corporate network access to automate key business to business (B2B) processes. While a contract may be in place between the third-party vendor and company to ensure the vendor has proper security measures in place, this might not be enough to safeguard your corporate network and systems. Implementing a robust third-party risk management program can help you prevent intrusions.

Typical External Third-Party Vendor Access



Security leaders should strive at all times to match the threats and their capabilities to their responses.

How Do We Evolve with the Threats?



There are two main controls to dealing with threats. 1) The noise to detect – what controls do you have in place to improve your chances of detecting the digital noise made by anattacker? 2) The difficulty of compromise – what controls do you have in place to increase your defense or raise the height of the wall? In other words, are you making it harder for bad guys to get in, therefore reducing the number of bad guys that access your network? Always ask yourself how you are addressing these two main controls and, where these controls intersect or get close to intersecting, consider the operating surface of the bad guy and where your response and strategic focus should be.

Corporate entities continue to play a "cat and mouse" game with adversaries seeking to attack systems and acquire assets. According to a study by the RAND Corporation, black and gray markets for computer hacking tools, services and byproducts continue to represent a threat to businesses, governments and individuals.

RAND Analyst Lillian Ablon describes the current climate: "Hacking used to be an activity that was mainly carried out by individuals working alone, but over the last 15 years the world of hacking has become more organized and reliable. In certain respects, cybercrime can be more lucrative and easier to carry out than the illegal drug trade."

As an example of how quickly stolen assets can be monetized, consider the December 2013 breach of the retailer, Target. Within days of the data hijack that affected nearly 70 million user accounts – those accounts were made available for purchase on black market websites. This example is hardly a-typical. The sophistication of the grey and black markets for data are such that information that is harvested can be sold and resold many times over before its value is exhausted. (Holt, March 2014)

Force 5: Government and Industry Regulations

Government and industry regulations frequently change and impact every business sector to varying degrees. Most security professionals understand that compliance doesn't equal security, but the business link between budget and compliance too often leaves security organizations leaning on regulatory requirements to drive security programs. Unfortunately, many security programs that focus on compliance fall short of providing a framework for an effective security program.

Let's look at some regulatory requirements and their security program shortfalls:

- GLBA – requires that organizations protect financial account data, but does not address most forms of privacy-related information or intellectual capital. GLBA is not as prescriptive as many of the other regulations on actions that organizations must take to comply with the legislation.
- PCI – was designed to protect cardholder data, but was not intended to be a complete security framework. Companies are spending entire annual IT security budgets on point solutions to address specific elements of the Data Security Standard. Unfortunately, with all of these requirements and costs, many other security program elements are pushed aside, leaving much of the company's sensitive data (not related to cardholder information) without a risk-based security posture.
- HIPAA – protects personal healthcare information (PHI) used in a patient's care and treatment. Similar to PCI, the HIPAA regulations focus on PHI and ignore other sensitive information that organizations need to protect. HIPAA does support a risk-based approach to security, and recognizes the fact that smaller organizations may not be able to implement the more advanced controls. The HIPAA Enforcement Rule, HIPAA "wall of shame", and recent updates to the Omnibus rules provide insight into non-compliance penalties.
- Sarbanes-Oxley (SOX) Section 404 – assesses the effectiveness of internal controls around financial information, but beyond this scope, the security environment is largely ignored. SOX was the first legislation to include civil and criminal penalties for non-compliance.
- Country Privacy Laws - privacy laws around the world that organizations must consider when designing a security strategy.

Force 5: Government and Industry Regulations

To understand the impact of Government and Industry Regulations, ask:

› What industry and government regulations apply to your organization?

› Can your organization adopt a strategy that minimizes the scope of the regulations?

› Can your organization implement controls that satisfy compliance and security functions?

› Are there changing regulatory requirements that will impact your organization?

› Is your business expanding into a market that has new regulatory requirements?

› Are there privacy laws that govern the use, consent and proper disclosure of personal information? Do you have a chief privacy officer that is responsible for compliance of the non-IT requirements of the regulations?

› How is your relationship with your legal and compliance teams? Do you have regular meetings with them to discuss the requirements of existing regulations and the possible business impact of new regulations?

> The EU Data Protection Act has been leading the world on governing the use and protection of personal data. Various countries around the globe have implemented privacy laws that protect the use, consent and disclosure of personal data. Many of these laws protect citizens regardless of whether or not your organization conducts business in that country.

Far too many regulations impact security programs than can be covered in this white paper. Multinational companies must understand and comply with privacy laws within the countries in which they conduct business. And, U.S. businesses need to be aware of state and local laws. For example, Massachusetts, Nevada and other states have privacy laws that protect their citizens.

With all these competing demands, many companies spend incredible amounts of money to achieve compliance, focusing on the checklist of required controls to avoid fines and reputational stigmas. Unfortunately, in addressing the specific goals of a specific regulatory requirement, organizations are not focused on implementing a complete and well-functioning security program. As such, regulatory requirements should not be the foundation on which you base your security strategy. They should, however, be an ongoing consideration, and a complete security program should result in compliance. You must be aware of applicable regulations as well as the challenges created through those regulations, and constantly keep abreast of new requirements that could impact your business and security strategy. Businesses that do not comply with regulations run the risk of being investigated and fined, or otherwise punished. Effective security leaders consider the information risk to their organizations, regardless of the regulatory requirements.

For most enterprises, regulatory compliance should be treated like a risk that needs to be mitigated like any other. It should not be viewed as a roadmap that a company can follow to improve security.

At best, regulatory mandates are often a useful tool in persuading senior leadership to support security initiatives. Privacy laws are rapidly changing within the United States and around the world. Understanding how this force impacts the information security strategy is a must for CISOs to be successful.

Force 6: Global Social and Political Forces

Changes in the global geo-political landscape or the global economy can have a significant impact on information security strategy. You must consider the potential security risks posed by a country's stability, economic outlook or geo-political viewpoint, just as enterprises that conduct business internationally must take such political and economic factors into account in their planning.

Geopolitical instability is one of the most common risks but there are others. Nascent copyright laws, developing international law systems, corruption and an unstable business economy can all be considered as potential risk factors. Dissent and state-sponsored malicious activity has also been proven to lead to outbreaks of cybercrime.

In other cases, developing nations may turn a blind eye to companies that steal data from their political and economic competitors. Any company doing significant international business may be confronted with government-sanctioned, if not government-sponsored, espionage. Successful attacks have targeted diplomatic communications, business negotiations and intellectual property – placing any targeted organizations at a competitive disadvantage.

Security strategy needs to account for economic pressures, as the global economy can change the behavior of foreign suppliers, which may choose to cut costs during locally slow economic periods. Spending on security is often a prime area for cost cutting, forcing the supplier – and its customer – to accept more risk. Understanding the geo-political and economic conditions not on the markets where the enterprise is selling product, but the nations in which its suppliers do business, will result in a more business-aligned security strategy.

You should also be aware of unrest and dissidents in other countries. Organizations need to gauge the likelihood that they will be a target for online protests, whether from a group associating itself with global protest movements or a regional activism community. Companies that sponsored the Federation Internationale de Football Association (FIFA) World Cup 2014, for example, became the targets of digital protesters in Brazil and worldwide, who were critical of the enormous costs of the games in a country where basic needs are often unmet.

A good security strategy will seek to identify and mitigate potential reputational – and possibly, informational – risks.

Force 6: Global Social and Political Forces

To understand the impact of Global Social and Political Forces, ask:

- In what other countries do your organization's branch offices, customers or suppliers reside?
- Do the countries with which your organization does business have laws that support the security of your organization's data and business?
- Can your organization exclude countries that are not supportive of modern business practices?
- Is your organization involved with or conducting business with Nation States?
- Does your organization engage in business that is controversial? Are there organizations in various countries that might target your organization?
- Are you outsourcing the development of a new product in a country that does not support copyright law?

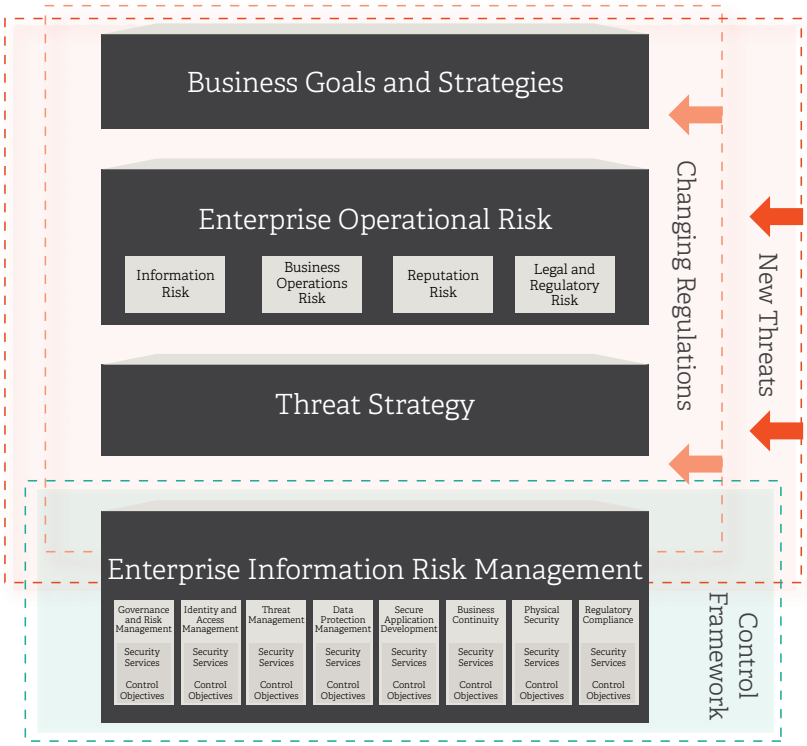
Using the Forces to Formulate a Strategy

Optiv's Six Forces of Security Strategy provides you with the considerations you must take into account when building a security strategy. Any strategy should guide business leaders in making decisions that align with your organization's goals. The strategy translates into a security program that assesses the security posture, identifies assets and gauges the risks. It is essential that you constantly monitor for changes in the six forces and adapt your security strategy to promote maximum business alignment.

As a security leader, you should gain support by discussing security in the context of helping your organization, not by using fear, uncertainty and doubt (FUD). The security practitioner that consistently points to the danger and risks inherent in adopting any technology or revamping any business practice without offering mitigations or alternatives is often ignored. A good way to assess your organization's security maturity is to understand how the organization approaches risks and responds to threats.

Once you've completed your security strategy, it is possible to create a security program. The program is the roadmap to implementing the security strategy and drives the changes in people, process and technology to enable the security services. This roadmap includes implementation of security technologies and evaluation of their performance in attaining the goals identified in the security strategy.

As a security leader, it's important that you resist the urge to view risks through the lens of available security technologies, and point-in-time threats. In some cases, appropriate processes and scope reduction can allow your organization to jettison a security technology that otherwise may have appeared necessary. You should also focus on building communities of like-minded security experts. Such communities can share functional practices, identify new threats and aid with incident response.



Conclusion

Far too few enterprise-level organizations have considered, much less created, a security strategy. Using Optiv's Six Forces of Security Strategy enables your organization to avoid defaulting to a compliance-driven approach to define your security program. Compliance-drive approaches have proven ineffective for protecting organizations' key information assets. Yet, such cookie-cutter programs typically lead to a one-size-fits-all security program based on the most common security technologies and not on effective means to reduce risk for the business.

Business studies, such as those by Michael Porter, defined forces of competition and sought to find common ground across industries where business leaders believed none existed. Optiv's Six Forces of Security Strategy is a vehicle for security leaders to identify the essential characteristics of their business environments and illuminate how those characteristics impact the organization's approach to security. While every organization needs to deal with the same six forces, the impact of the various forces is unique to each organization and can result in dramatically different approaches to security.

In the end, the creation of a security strategy – and its subsequent transformation into a security program – is not a single destination but a journey. Along this journey, security leaders need to continually reevaluate the organization's strengths, weaknesses and goals, while aligning security measures appropriately to foster business growth.

The security practitioner that consistently points to the danger and risks inherent in adopting any technology or revamping any business practice without offering mitigations or alternatives is often ignored.

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

10.15 | F1