MicroStrategy Usher:
A maturity model for enterprise security.
Today, organizations are facing a challenging and constantly evolving landscape of security threats. Supercharged connectivity, unending streams of information and instantaneous transactions have created unprecedented opportunities for business—but they also create vulnerabilities. Cyber threats continue to target organizations of every size and type around the world, making the need for enterprise security more urgent than ever.

Yet many organizations are still reluctant to commit sufficient resources to security, failing to recognize that now, more than ever, security is a critical business competency. Perhaps among the reasons for recent prominent information security breaches is the lingering mentality among business leaders that security is a costly, superficial accessory. These high-visibility cyber-attacks on global corporations drive home the need for more holistic thinking about security and risk management. To meet today's security challenges, organizations must begin to think about security in a business context.

But how do organizations go about this process, and what does it actually look like in practice? This paper presents a framework for thinking about security maturity and profiles the four stages that organizations advance through as they deepen their security capabilities. The goal of this paper is to help organizations assess their level of security maturity in a larger context in order to inform business decisions.

The four phases of organizational security maturity

The evolution of how organizations regard information security

Every organization has unique tolerances and expectations about how security interacts with their company. These expectations depend on many factors, including industry, regulations, and perceived threats. Going from left to right, the chart above categorizes security maturity in four phases, moving from an immature company in the “checklist” phase, right up to those who are doing “business risk” security, understanding the business risk in a corporate-wide context. This process is largely defined by how closely security is integrated into the core business strategy of an organization, and is best signified by the position of the chief information security officer (CISO) and how closely he or she works with business and IT leadership. Each stage of the security maturity process is outlined in the sections below.
Phase I: Checklist

Phase I is known as the checklist phase because companies at this point will create and closely adhere to a list of security must-haves, a well-defined checklist. Checklist items typically include enterprise-class antivirus, intrusion detection systems, firewalls, and strong authentication for employees. At this stage, security is rarely a serious business priority. The security team is most likely an isolated department that operates according to its own set of rules and is not very engaged with the rest of the business. The CISO likely doesn’t have a “seat at the table” in terms of central business strategy.

Checklist items aside, organizations in this phase focus on initiatives that will succeed politically and generate visible business value, such as engines on the backend that help with auditing. Some companies will begin to adopt codes of practice, or information security standards, in this phase. There are numerous frameworks that organizations may pursue, depending on their industry and geographic location. These may include ISO 27001, 27002, BS 1779, COBIT, etc. Without hard regulations, however, there is often little motivation for companies to move out of Phase I, as the business decision makers emphasize ease of use.

Phase II: Compliance

Moving past the checklist phase, organizations graduate into Phase II, a regulation-driven phase. Graduating to this phase is typically catalyzed by the passage or strengthening of industry rules and regulations by legislative bodies, industry groups, or consumer advocacy groups.

Some prominent examples of regulations with security provisions:

- Sarbanes-Oxley Act (SOX): requires that public companies guard their data to ensure that financial reports are not based on tampered numbers
- Federal Financial Institutions Examination Council (FFIEC): requires multifactor authentication for online banking
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada): requires customer consent to collect personal data, and data can only be used for the purpose for which customers give consent

Security maturity rises rapidly in the early stage of this phase, but then plateaus when businesses reach compliance. Maturity will rarely go beyond close compliance with the regulations at hand. In this phase, cost becomes the main issue. If the downsides of noncompliance, such as potential losses from a breach or regulatory fines, don’t outweigh the cost to implement, then it is unlikely a company will aim for compliance (and vice versa). Effectively, when companies address security as a response to more prescriptive and more punitive regulations, security becomes a compliance function.

Because of this, regulations sometimes need to be revised to drive increased levels of compliance, and therefore, security maturity. For example, when HIPAA’s patient privacy regulations were initially enacted, the fine for a violation was capped at $100 per incident, with a maximum of $25,000 per year. To be compliant, organizations had to, among other things, deploy network intrusion detection systems (IDS). The associated $25,000 annual implementation and maintenance cost resulted in low compliance, as it was more cost-effective to simply pay the fine. Therefore, a new penalty structure was implemented in 2009 by which the ceiling for fines was raised to $50,000 per incident, with a maximum of $1,500,000 per year.

On the other hand, some regulations are crafted with positive compliance incentives. Basel I, II, and III, a series of banking requirements, stipulate that if a financial institution implements a risk-based management scheme, then it may hold a lower cash reserve ratio. Suddenly, the lines of business will care about security, as it affects the profit and loss statement.

What types of organizations are experiencing Phase II? Right now it is primarily retailers, healthcare providers and services, and smaller banks and financial institutions.

Phase III: An IT Risk

Once regulatory controls are imposed on an industry, the next step in security maturity is the IT risk phase. The new IT infrastructure required for compliance in Phase II gives information security professionals, like the directors of information security (InfoSec) and the CISOs, the opportunity to work more closely with business people. In Phase III, IT and business work together to mitigate risk inherent in IT systems, repositories of sensitive data, and valuable information. The organization will begin to understand how to articulate risk in an IT context as it moves towards developing better up-to-the-minute situational awareness about both physical and logical systems and supporting infrastructure.
Security maturity will gradually grow in Phase III. Routine tests on security metrics will be common in this phase, though they may have been initiated in Phase II. In this phase, companies are concerned about assessing and minimizing IT risk, which is the potential that a given threat will exploit vulnerabilities of an information system and thereby cause harm to the organization. IT risk is measured in terms of a combination of the probability of occurrence of an event and its consequence ($\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value}$). Therefore, the security organization is less concerned about the number of incidents or viruses, and more about building a sound overall topography when it comes to information security. As a result, CISOs typically begin to be taken much more seriously in the business organization and communication between the security team and the business leaders may be more frequent.

Phase III is where companies may deepen security capabilities by building a Security Operations Center (SOC) or a Computer Incident Response Center (CIRC). SOCs ensure security controls are functioning correctly and configured according to business need. They also make sure threats and incidents are detected and responded to before they impact the business. Large financial services companies are prominent in the IT risk phase, having progressed through the checklist and compliance phases in the 2000s.

**Phase IV: Business Risk**

Once an organization matures beyond just dealing with IT risk, the divide between security thinking and business thinking begins to soften. This leads to Phase IV, known as the business risk phase. In Phase IV, security metrics are assessed for business impact. Customer satisfaction, revenue, cost, brand — they are all regarded in security terms. These companies think of IT risk as synonymous with business risk; in other words, IT risk isn’t confined to IT or the security practice, it is actually equal to and described in the same language as financial, operational, and legal risk. This is where security “grows up” and InfoSec becomes a pillar of central business strategy. This can be reflected in companies where the CISO reports to the board, or directly to the CEO, as opposed to just the CIO.

For companies to reach this phase, their security plans must contain elements that appeal to business management and speak to broader business concerns. They must align with the CEO’s priorities, such as driving revenue up, reducing costs, minimizing risk, boosting productivity, and advancing corporate strategic goals. In effect, this shifts the conversation from a security conversation to a business conversation. That way, organizations can overcome the traditional structural divide between IT (and thus security) and the business, a barrier that has plagued CIOs for decades.

Phase IV is the most mature level for a company. In general, these are companies that are deeply interested in the business impact or business risk of security, and are willing to invest more heavily in integrated, comprehensive security infrastructures. The defense industry has led the foray into Phase IV, as well as cutting-edge financial services companies, including some of the world’s largest investment banks.

**Conclusion**

Ultimately, sponsorship and buy-in from executive leadership is the deciding factor for achieving security maturity. With the right support, resources, and visibility, an organization can progress quickly towards a more secure future. More organizations around the world are realizing this, and as a result, involvement by senior executives continues to grow. Holistic approaches to security are gaining traction across more industries.

But in addition to executive buy-in and technological innovation, increasing the cybersecurity awareness of the workforce is equally important to achieving security maturity. Organizations need to establish understandable and measurable policies that reflect the organization’s unique corporate, threat, and regulatory circumstances, and this information needs to be disseminated in order to maintain top-to-bottom vigilance. By cultivating a “see something, say something” culture, companies foster organizational transparency, critical because an individual employee can be either the greatest ally or the biggest threat to security.

As shown in these four phases, structural forces, both within and outside of organizations, are often the main determinants of organizational maturity security. But that doesn’t have to be the case. Organizations should proactively incorporate security into the core of their strategy by aligning security, IT, and business units. To begin, organizations must assess their current security maturity to determine what may be holding them back from achieving more. Is it a lack of executive sponsorship? Is it a deeply entrenched divide between security and the rest of the business? Or is it prohibitive costs? The first step in solving these problems is to begin a dialogue between business and security leaders. That conversation should start today.