Once upon a time, risk management was a relatively calm area of organizational life. Management made sure that employee-, customer- and product-safety measures were in place. Controls and safeguards deterred theft and fraud. The regulatory environment was relatively stable. Organizations insured against losses and employed hedging, diversification and other time-tested risk management tools.

Most organizations understood the risks they faced and addressed them with fairly reliable approaches. Risks could be quantified, losses could be remediated and senior executives could sleep at night.

**Times have changed.**

In recent years, the volume and velocity of change have rendered risks far more numerous and complex. Risks have multiplied as business models and methods, information and communication technologies, and laws and regulations have become more complex. Add to that the globalization of markets, supply chains, innovation and crime, and you have a transformed risk environment.

As a result, today’s risks can be hard to identify and quantify, harder still to avoid, and intertwined with formerly unrelated risk areas. An operational risk event can ignite a reputational risk that generates a financial risk — a firecracker string of follow-on impacts.

In general, this environment calls for a series of shifts in management’s approach to risk:

- From largely compliance-based methods to more strategic approaches
- From backward-looking approaches to more forward-looking postures
- From reactive responses to proactive risk management
- From a focus only on value protection to a focus that includes value creation

Organizations need broader, deeper, more dynamic and holistic risk management approaches. The competitive, technological and regulatory environments demand it, as do customers, suppliers, investors and other stakeholders.

**Consider cyber risk**

The digitization of currencies, transactions, relationships, experiences and assets has transformed entire industries. Cyber — the whole world of digitized data, information and communications — is the great enabler. Think retail and the web, financial services and mobile phones, health care and wearable technologies, to name a few.

In the private and public sectors, and in financial services, life sciences, and other industries, cyber capabilities extend organizations’ borders and reach, creating new customers, business partners, avenues of access, methods of innovation and forms of value. As the great enabler, cyber generates myriad opportunities and risks.

Bringing the organization’s cyber risk management capabilities up to the level of its cyber capabilities now ranks among senior management’s chief priorities, for three reasons.

1. **Enhanced cyber risk management boosts growth and performance.** The better the cyber risk management program, the more the organization can leverage cyber capabilities for growth and performance. This calls for aligning cyber risk management with business strategy.

2. **Current methods fail to meet most organizations’ needs.** The prevailing point-specific, IT-centric, compliance-focused approaches to cyber risk management generate costs, gaps and overlaps while failing to adequately address exposures. The alternative is to integrate cyber risk controls with business processes.

3. **Management needs to evaluate cyber risks and outcomes.** Countermeasures tend to be deemed either effective or ineffective, with rudimentary — if any — analysis of related investments, outcomes and returns. The alternative is to target desired results and measure actual outcomes related to cyber risk exposure and invest accordingly.

Most organizations already possess many useful elements of a cyber risk management program. For example, policies, firewalls, access management tools and third-party due diligence hold a key place in a cyber risk program. Linkage with an organization’s IT strategy also plays an essential role. Regulatory compliance remains as important as ever. Yet a lack of an aligned, integrated and measurable cyber risk management program renders most cyber risk initiatives inadequate, inefficient or both.
Are you making these mistakes?
The approach most organizations take to cyber risks leads to common mistakes.

• Letting fear set the agenda. Cyber breaches can result in costly losses and embarrassing headlines. However, fear of breaches can focus management exclusively on point-specific, IT-centric solutions. While key, these solutions are regularly leapfrogged by cybercriminals and do not constitute a cyber risk management program. While a good dose of fear can be healthy, an overdose can be lethal.

• Undervaluing digital assets. Undervaluation of digital assets typically results from the absence of a rigorous digital asset valuation exercise. Executives know that noncompliance creates regulatory consequences, breaches cost money and denial of service attacks lose customers. But do they grasp the true value of all intellectual property in digital form? Do they understand the full costs of operational, financial, legal and reputational risks that stolen data, compromised transactions and corrupted systems can generate?

• Underpreparing for cyber incidents. Cyber incidents include not only external attacks, but also internal breaches, natural disasters and other events that affect systems and data. Given that cybersecurity can never be complete, management must be prepared to respond to any cyber incident. Sound preparation depends on the involvement of forensic, communication, legal and other experts, and must include regular updates to response plans as well as periodic drills.

• Adopting cyber capabilities without enough strategic context. Mobile devices, social media, cloud computing and artificial intelligence present risks and opportunities, just like vendor alliances, outsourcing, co-sourcing and joint venture arrangements. Management must understand the risks and rewards of any technology the organization employs, as well as the ways that cyber risks affect stakeholders and the pursuit of the business strategy.

The importance, ubiquity and value of cyber capabilities call for ongoing C-suite attention to cyber risk management. Cyber risk management should occur within a well-designed, properly implemented risk management and risk governance program that aims to manage the risks that attend value creation as well as those addressed in value protection.

A holistic approach
A holistic approach to cyber risk management enables management to:

• Place cyber risks in a strategic context. Treating cyber risk apart from other business risks renders it overly technical, mysterious and separate. Placing it in a strategic context shows how cyber risk relates to other risks. It also shows how management’s acceptance of specific cyber risks will assist — or fail to assist — in creating value. Perhaps most important, a strategic approach will focus all senior managers on defining and meshing their interests and roles in cyber risk management, enabling them to make explicit cyber risk management decisions.

• Link cyber risks to growth and performance. There’s no point in taking risks that don’t drive value creation. Most initiatives will present some cyber risks. To grasp the whole picture, management must address cyber risk in the context of strategic business goals. Management must also identify unrewarded cyber risks, which can occur, for example, when information about job responsibilities or internal systems is disclosed in job postings or on social media with no real payback.

• Rationalize practices and spend. A holistic approach enables management to move beyond point-specific, siloed, compliance- and IT-driven solutions to gain an integrated view of cyber risk management. It rationalizes practices, revealing overlaps, gaps and issues to be addressed, which enhances efficiency and effectiveness. Rationalizing practices — and investments — also means linking them to strategic goals, and weighing whether the goals warrant the risks and the risks serve the goals.

• Make better business decisions. Placing cyber risks in context and rationalizing practices should position the organization to better manage cyber risks. Management can evaluate cyber risk issues more precisely, deciding which to accept, which to avoid, and which to mitigate and to what extent. This also enables management to discern insurable and uninsurable risks. The resources needed to manage cyber risks can also be identified — talent, technology, funding or external assistance.
A holistic approach is best organized by means of a framework that helps management identify roles, responsibilities, relationships and other relevant factors (Cyber risk management framework). Grant Thornton LLP has developed this framework to assist in defining enablers of cyber risk management, elements of a cyber risk management program and expected outcomes of such a program. These three considerations must be analyzed in the context of the organization’s industry and business.

Cyber risk management framework

<table>
<thead>
<tr>
<th>Business enablers</th>
<th>Program elements</th>
<th>Business outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business acumen</td>
<td>Governance</td>
<td>Assets protected</td>
</tr>
<tr>
<td>Business strategy</td>
<td></td>
<td>Competitive advantage</td>
</tr>
<tr>
<td>Leadership</td>
<td>Assets</td>
<td>Stakeholders’ confidence</td>
</tr>
<tr>
<td>Digital strategy</td>
<td>Third-party data</td>
<td>Compliance</td>
</tr>
<tr>
<td>Regulations/compliance</td>
<td>Confidential information</td>
<td>Reputation maintained</td>
</tr>
<tr>
<td>Resources</td>
<td>Vendor data</td>
<td>Resilience</td>
</tr>
<tr>
<td>Enterprise risk management</td>
<td>Customer data</td>
<td>Continual improvement</td>
</tr>
<tr>
<td></td>
<td>Employee data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intangibles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partner data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PCI/PI/PHI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technology</td>
<td></td>
</tr>
</tbody>
</table>

Within each of the three columns — enablers, program elements and expected outcomes — are, respectively, factors that enable the program, constitute the program, and target and measure outcomes of the program.

- **Enablers** (i.e., business acumen, business strategy, compliance demands and resources) determine the need for cyber risk management, inform the nature of the program and help define its elements. Thus cyber risk program management will vary not only from industry to industry but among organizations within an industry.

- **Program elements** (i.e., governance, assets, processes and technology that comprise the program) will also vary from organization to organization and over time as strategies and needs evolve. Key elements include the digital assets to be secured and the processes and technologies for securing them, which underscore the essential role of IT.

- **Expected outcomes** encompass asset protection and compliance as well as outcomes associated with value creation (i.e., competitive advantage, stakeholders’ confidence and continual improvement).

Drilling down on any element of the framework enables management to assess that factor and its current and target role in the cyber risk management program. With target roles defined and prioritized, the organization can then work to enhance cybersecurity and cyber risk management in a balanced, coordinated manner that addresses the most important and urgent needs.
AIM — an approach to cyber risk management

To assist in developing a holistic approach to cyber risk management, we have developed a three-step iterative approach called AIM (The AIM approach).

The AIM approach

- **Align:** When management aligns risk management with the business strategy, they ensure that the organization only accepts risks that support business and performance goals. This step broadens analysis of cyber risk and cybersecurity decisions and investments by examining ways in which they support — or fail to support — strategies and goals.

- **Integrate:** Alignment sets the stage for integration of cyber controls with business processes, enabling management to move beyond point-specific and compliance-based solutions while recognizing that they have their place. An integrated approach leverages processes, people and technologies across businesses, functions and activities within a well-structured risk management and governance program. Done properly, integration also identifies metrics to ensure ongoing alignment and effectiveness.

- **Measure:** Measuring the outcomes, costs and returns on the cyber risk management program enables management to see what is working and what isn’t, identify needed (and unneeded) resources, rationalize investments and pursue continuous improvement. Although they can be hard to quantify, cyber risks — and their costs and impacts — can indeed be measured and addressed in an organized manner.

AIM not only establishes context, but also methods of approaching key cyber risk management tasks, including ways to:

- Identify and evaluate a broad range of digital assets and cyber risks
- Gauge the value of digital assets and dangers of specific cyber risks
- Decide what to monitor, how to monitor it, and how to set policies, procedures and thresholds
- Analyze existing and potential countermeasures, including how much insurance to buy, third-party due diligence, and technological and behavioral steps
- Understand what internal and external resources are available to the organization and how they should be allocated
- Establish a true cyber incident response program, including detection, containment, forensics, communications, recovery and remediation procedures
- Develop and implement a phased-in cyber risk management program equal to the cyber risks that the organization faces

With the AIM approach, IT becomes a critical part of the solution rather than the solution, and management, risk experts and IT specialists can more effectively identify, analyze, measure and address cyber risks.
Cyber risk factors

Relative to other business risks, cyber risks present several specific challenges.

- **Cyber risks are ubiquitous and hard to identify and quantify.** Unlike credit, investment and other risks, cyber risks expose the organization and its stakeholders in ways that can be difficult to imagine. Therefore, many organizations incur cyber risks unwittingly and for no strategic reason.

- **Digital assets can equal or exceed the value of physical assets.** Customer and supplier data, bank and investment accounts, personal information (e.g. on executives and directors), deal details, strategic plans and intellectual property all have value. That is why cybercriminals target organizations through outright theft, ransomware and other tactics.

- **Total cybersecurity cannot be achieved.** Organizations are too porous and dependent on cyber capabilities — and have too many internal and external stakeholders with system access — for total cybersecurity to be achievable.

- **Reactive, point-specific solutions are incomplete.** Obviously, an organization must control access, erase lost devices, respond to attacks and take other standard cybersecurity steps. But cyber risk management and those steps must serve the larger risk management strategy and operate in a strategic context.

- **A strategic approach increases security.** While cybersecurity can never be complete, a strategic approach to cyber risk management holds several benefits. It will cover a broad range of cyber risks, improve visibility into cyber risks, enhance cyber risk decision-making, promote efficient compliance and reporting, and assure stakeholders that management has cyber risks covered.

**Steps to consider**

Organizations take cyber risks for the same reason they take other risks — to create value. But because cyber risks can be hard to identify and quantify, management may fail to fully appreciate them. When that happens, the organization takes risks that may be unknown and unmanaged, and that’s a recipe for value destruction.

To counter that tendency, consider these steps.

- **Map business processes, stakeholders and related data and systems.** It’s easy to think of digital assets as residing “on the computer” or “in the cloud” but the digitization of business generates data flows with high value — if only in the event they are compromised. Mapping business processes, stakeholders, and data and systems to your strategies and goals will identify cyber risks and the other risks they can drive. Doing so will also help to relate risks to strategies and identify desired modifications to the strategy and investments.

- **Know that regulatory compliance is necessary, but not sufficient.** Regulatory standards tend to address known risks (just as generals tend to fight the last war). While necessary, achieving compliance will not defend against malware, ransomware or other methods currently being developed by cybercriminals. Compliance must be accomplished effectively and efficiently, but it mainly addresses compliance risks — not the full range of cyber risks.

- **Evaluate strategic digital, as well as physical, assets.** A jewelry company may store its precious gems and metals in a vault, but fail to secure its digital records and financial accounts. The impact of the cyber risks could outweigh those of physical theft. It’s easy to undervalue internal emails, deal details, strategic plans and intellectual property.
• Don’t confuse a cyber risk management program with ERM. Enterprise risk management (ERM) systems often incorporate aspects of suboptimal approaches to cyber risk. They can be point-specific and siloed, piecemeal and reactive, compliance- and IT-centric, and inadequate. ERM systems typically focus on data, systems and compliance without taking a holistic approach. ERM plays a role in cybersecurity, but it should not be mistaken for a cyber risk management program.

• Start the cyber risk conversation. Cyber risk permeates the organization, giving every senior executive of a business or function a stake in cyber risk management. Each also has a role in and responsibility for the success (or failure) of the organization’s cyber risk management program. For that reason, any senior executive can initiate a broader, deeper conversation about cybersecurity.

For most organizations, the latter element may be the most important. Cybersecurity must be developed and implemented in the context of a well-funded, well-coordinated, enterprise-wide cyber risk management program. The conversation that will generate and sustain that program has to begin at the top and be supported through continuing senior executive engagement.

CASE STUDY

Global asset management firm

THE SITUATION
The firm had invested heavily in cybersecurity tools, but management still lacked comfort regarding cyber risks. These risks included potential regulatory breaches, service failures, business disruptions, third-party exposures, and loss of client data and intellectual property, such as trading strategies.

WHAT THE TEAM DID
Grant Thornton worked with the organization to:
• Evaluate digital and system assets to prioritize those most critical to the firm’s strategies, competencies and success
• Identify risks specific to the firm’s asset classes, regulatory expectations and business initiatives (such as a move to offer robo investing)
• Design a risk management framework related to the locations and timing of cyber risks
• Develop a cyber risk management and monitoring program, including a cybersecurity monitoring program for third parties

OUTCOMES
This was the first time the firm had undertaken a business-focused approach to cyber risk. As a result, management:
• Rationalized cybersecurity investments and aligned them to key cyber risks rather than simply applying tools
• Consolidated relationships among business units and system vendors to achieve savings and conformity in cybersecurity solutions
• Became more directly engaged in cyber risk management and risk-related CIO support
About Grant Thornton LLP
Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world’s leading organizations of independent audit, tax and advisory firms. In the United States, Grant Thornton has revenue in excess of $1.3 billion and operates 58 offices with more than 500 partners and 8,000 employees. Grant Thornton works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations.

This content is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information about the issues discussed, contact a Grant Thornton LLP professional.

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the GTIL member firms provide audit, tax and advisory services to their clients, as the context requires. GTIL and each of its member firms are separate legal entities and are not a worldwide partnership. GTIL does not provide services to clients. Services are delivered by the member firms in their respective countries. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. In the United States, visit grantthornton.com for details.

© 2016 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd