[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@3d38244f2b1b4256882990d9b2ccc0d8?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

ref <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity>

**The risk-based approach to cybersecurity**

                                            October 8, 2019                         | Article

        By [Jim Boehm](https://www.mckinsey.com/our-people/jim-boehm), Nick Curcio, Peter Merrath, Lucy Shenton, and Tobias Stähle                *Open interactive popup*                                                             The risk-based approach to cybersecurity            *Open interactive popup*

            The most sophisticated institutions are moving  from a “maturity based” to a “risk based” approach for managing  cyberrisk. Here is how they are doing it.

**Top managers at most companies** recognize cyberrisk  as an essential topic on their agendas. Worldwide, boards and executive  leaders want to know how well cyberrisk is being managed in their  organizations. In more advanced regions and sectors, leaders demand,  given years of significant cybersecurity investment, that programs also  prove their value in risk-reducing terms. Regulators are challenging the levels of enterprise resilience that companies claim to have attained.  And nearly everyone—business executives, regulators, customers, and the  general public—agrees that cyberrisk is serious and calls for constant  attention (Exhibit 1).

      Exhibit 1                                                                                            We strive to provide individuals with  disabilities equal access to our website. If you would like information  about this content we will be happy to work with you. Please email us  at: [McKinsey\_Website\_Accessibility@mckinsey.com](mailto:McKinsey_Website_Accessibility@mckinsey.com)

What, exactly, organizations should do is a more difficult question.  This article is advancing a “risk based” approach to cybersecurity,  which means that to decrease enterprise risk, leaders must identify and  focus on the elements of cyberrisk to target. More specifically, the  many components of cyberrisk must be understood and prioritized for  enterprise cybersecurity efforts. While this approach to cybersecurity  is complex, best practices for achieving it are emerging.

To understand the approach, a few definitions are in order. First,  our perspective is that cyberrisk is “only” another kind of operational  risk. That is, cyberrisk refers to the potential for business losses of  all kinds—financial, reputational, operational, productivity related,  and regulatory related—in the digital domain. Cyberrisk can also cause  losses in the physical domain, such as damage to operational equipment.  But it is important to stress that cyberrisk is a form of business risk.

Furthermore, cyberrisks are not the same as cyberthreats, which are  the particular dangers that create the potential for cyberrisk. Threats  include privilege escalation, vulnerability exploitation, or phishing.    1  Cyberthreats exist in the context of enterprise cyberrisk as potential  avenues for loss of confidentiality, integrity, and availability of  digital assets. By extension, the risk impact of cyberthreats includes  fraud, financial crime, data loss, or loss of system availability.

Decisions about how best to reduce cyberrisk can be contentious.  Taking into account the overall context in which the enterprise  operates, leaders must decide which efforts to prioritize: Which  projects could most reduce enterprise risk? What methodology should be  used that will make clear to enterprise stakeholders (especially in IT)  that those priorities will have the greatest risk reducing impact for  the enterprise? That clarity is crucial in organizing and executing  those cyber projects in a focused way.

At the moment, [attackers benefit from organizational indecision on cyberrisk](https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/defense-of-the-cyberrealm-how-organizations-can-thwart-cyberattacks)—including the prevailing lack of clarity about the danger and failure to execute  effective cyber controls. Debilitating attacks on high-profile  institutions are proliferating globally, and enterprise-wide cyber  efforts are needed now with great urgency. It is widely understood that  there is no time to waste: business leaders everywhere, at institutions  of all sizes and in all industries, are earnestly searching for the  optimal means to improve cyber resilience. We believe we have found a  way to help.

**The maturity-based cybersecurity approach: A dog that’s had its day**

Even today, “maturity based” approaches to managing cyberrisk are  still the norm. These approaches focus on achieving a particular level  of maturity by building certain capabilities. To achieve the desired  level, for example, an organization might build a security operations  center (SOC) to improve the maturity of assessing, monitoring, and  responding to potential threats to enterprise information systems and  applications. Or it might implement multifactor authentication (MFA)  across the estate to improve maturity of access control. A  maturity-based approach can still be helpful in some situations: for  example, to get a program up and running from scratch at an enterprise  that is so far behind it has to “build everything.” For institutions  that have progressed even a step beyond that, however, a maturity-based  approach is inadequate. It can never be more than a proxy for actually  measuring, managing, and reducing enterprise risk.

**Most Popular Insights**

2. [When will the COVID-19 pandemic end?](https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/when-will-the-covid-19-pandemic-end)
4. [Defining the skills citizens will need in the future world of work](https://www.mckinsey.com/industries/public-and-social-sector/our-insights/defining-the-skills-citizens-will-need-in-the-future-world-of-work)
6. [COVID-19: Implications for business](https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/covid-19-implications-for-business)
8. [Back to the future? Airline sector poised for change post-COVID-19](https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/back-to-the-future-airline-sector-poised-for-change-post-covid-19)
10. [What’s going on with shipping rates?](https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/whats-going-on-with-shipping-rates)

A further issue is that maturity-based programs, as they grow  organically, tend to stimulate unmanageable growth of control and  oversight. In monitoring, for example, a maturity-based program will  tend to run rampant, aspiring to “monitor everything.” Before long, the  number of applications queued to be monitored across the enterprise will outstrip the capacity of analysts to monitor them, and the installation of monitors will bog down application-development teams. The reality is that some applications represent more serious vulnerabilities—and  therefore greater potential for risk—than others. To focus directly on  risk reduction, organizations need to figure out how to move from a  stance of monitoring everything to one in which particular applications  with high risk potential are monitored in particular ways.

Another issue related to the monitor-everything stance is inefficient spending. Controls grow year after year as program planning for  cybersecurity continues to demand more spending for more controls. But  is enterprise risk being reduced? Often the right answers lie elsewhere: for example, the best return on investment in enterprise-risk reduction is often in employee awareness and training. Yet a maturity-based model does not call for the organization to gather enough information to know that it should divert the funding needed for this from additional  application monitoring. Spending on both will be expected, though the  one effort (awareness and training) may have a disproportionate impact  on enterprise-risk reduction relative to the other.

If the objective is to reduce enterprise risk, then the efforts with  the best return on investment in risk reduction should draw the most  resources. This approach holds true across the full control landscape,  not only for monitoring but also for privileged-access management,  data-loss prevention, and so forth. All of these capabilities reduce  risk somewhat and somehow, but most companies are unable to determine  exactly how and by how much.

The final (and most practical) drawback of maturity-based programs is that they can create paralyzing implementation gridlock. The few teams  or team members capable of performing the hands-on implementation work  for the many controls needed become overloaded with demand. Their highly valuable attention is split across too many efforts. The frequent  result is that no project is ever fully implemented and program  dashboards show perpetual “yellow” status for the full suite of cyber  initiatives.

The truth is that in today’s hyperconnected world, maturity-based [cybersecurity programs](https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/perspectives-on-transforming-cybersecurity) are no longer adequate for combatting cyberrisks. A more strategic,  risk-based approach is imperative for  effective and efficient risk  management (Exhibit 2).

      Exhibit 2                                                                                            We strive to provide individuals with  disabilities equal access to our website. If you would like information  about this content we will be happy to work with you. Please email us  at: [McKinsey\_Website\_Accessibility@mckinsey.com](mailto:McKinsey_Website_Accessibility@mckinsey.com)

**Reducing risk to target appetite at less cost**

The risk-based approach does two critical things at once. First, it  designates risk reduction as the primary goal. This enables the  organization to prioritize investment—including in  implementation-related problem solving—based squarely on a cyber  program’s effectiveness in reducing risk. Second, the program distills  top management’s risk-reduction targets into precise, pragmatic  implementation programs with clear alignment from the board to the front line. Following the risk-based approach, a company will no longer  “build the control everywhere”; rather, the focus will be on building  the appropriate controls for the worst vulnerabilities, to defeat the  most significant threats—those that target the business’s most critical  areas. The approach allows for both strategic and pragmatic activities  to reduce cyberrisks (Exhibit 3).

Exhibit 3

Companies have used the risk-based approach to effectively reduce  risk and reach their target risk appetite at significantly less cost.  For example, by simply reordering the security initiatives in its  backlog according to the risk-based approach, one company increased its  projected risk reduction 7.5 times above the original program at no  added cost. Another company discovered that it had massively  overinvested in controlling new software-development capabilities as  part of an agile transformation. The excess spending was deemed  necessary to fulfill a promise to the board to reach a certain level of  maturity that was, in the end, arbitrary. Using the risk-based approach, the company scaled back controls and spending in areas where desired  digital capabilities were being heavily controlled for no risk-reducing  reason. A particular region of success with the risk-based approach has  been Latin America, where a number of companies have used it to leapfrog a generation of maturity-based thinking (and spending). Instead of  recapitulating past inefficiencies, these companies are able to build  exactly what they need to reduce risk in the most important areas, right from the start of their cybersecurity programs. Cyber attackers are  growing in number and strength, constantly developing destructive new  stratagems. The organizations they are targeting must respond urgently,  but also seek to reduce risk smartly, in a world of limited resources.

**A transformation in sequential actions**

Companies adopting the risk-based approach and transforming their  “run” and “change” activities accordingly inevitably face the crucible  of how to move from maturity-based to risk-based cybersecurity. From the experience of several leading institutions, a set of best-practice  actions has emerged as the fastest path to achieving this  transformation. These eight actions taken roughly in sequence will align the organization toward the new approach and enable the appropriate  efforts to reduce enterprise risk.

2. Fully embed cybersecurity in the enterprise-risk-management framework.
4. Define the sources of enterprise value across teams, processes, and technologies.
6. Understand the organization’s enterprise-wide  vulnerabilities—among people, processes, and technology—internally and  for third parties.
8. Understand the relevant “threat actors,” their capabilities, and their intent.
10. Link the controls in “run” activities and “change” programs to  the vulnerabilities that they address and determine what new efforts are needed.
12. Map the enterprise risks from the enterprise-risk-management  framework, accounting for the threat actors and their capabilities, the  enterprise vulnerabilities they seek to exploit, and the security  controls of the organization’s cybersecurity run activities and change  program.
14. Plot risks against the enterprise-risk appetite; report on how cyber efforts have reduced enterprise risk.
16. Monitor risks and cyber efforts against risk appetite, key cyberrisk indicators (KRIs), and key performance indicators (KPIs).

**1. Fully embed cybersecurity in the enterprise-risk-management framework**

A risk-based cyber program must be fully embedded in the  enterprise-risk-management framework. The framework should not be used  as a general guideline, but rather as the organizing principle. In other words, the risks the enterprise faces in the digital domain should be  analyzed and categorized into a cyberrisk framework. This approach  demystifies cyberrisk management and roots it in the language,  structure, and expectations of enterprise-risk management. Once  cyberrisk is understood more clearly as business risk that happens in  the digital domain, the organization will be rightly oriented to begin  implementing the risk-based approach.

**2. Define the sources of enterprise value**

An organization’s most valuable business work flows often generate  its most significant risks. It is therefore of prime importance to  identify these work flows and the risks to which they are susceptible.  For instance, in financial services, a loan process is part of a  value-creating work flow; it is also vulnerable to data leakage, an  enterprise risk. A payment process likewise creates value but is  susceptible to fraud, another enterprise risk. To understand enterprise  risks, organizations need to think about the potential impact on their  sources of value.

Identifying the sources of value is a fairly straightforward  exercise, since business owners will have already identified the risks  to their business. Cybersecurity professionals should ask the businesses about the processes they regard as valuable and the risks that they  most worry about. Making this connection between the cybersecurity team  and the businesses is a highly valuable step in itself. It motivates the businesses to care more deeply about  security, appreciating the bottom-line impact of a recommended control.  The approach is far more compelling than the maturity-based approach, in which the cybersecurity function peremptorily informs the business that it is implementing a control “to achieve a maturity of 3.0.”

The constituents of each process can be defined—relevant teams,  critical information assets (“crown jewels”), the third parties that  interact with the process, and the technology components on which it  runs—and the vulnerabilities to those constituent parts can be  specified.

**3. Understand vulnerabilities across the enterprise**

Every organization scans its infrastructure, applications, and even  culture for vulnerabilities, which can be found in areas such as  configuration, code syntax, or frontline awareness and training. The  vulnerabilities that matter most are those connected to a value source  that particular threat actors with relevant capabilities can (or intend  to) exploit. The connection to a source of value can be direct or  indirect. A system otherwise rated as having low potential for a direct  attack, for example, might be prone to lateral movement—a method used by attackers to move through systems seeking the data and assets they are  ultimately targeting.

Once the organization has plotted the people, actions, technology,  and third-party components of its value-creating processes, then a  thorough identification of associated vulnerabilities can proceed. A  process runs on a certain type of server, for example, that uses a  certain operating system (OS). The particular server–OS combination will have a set of identified common vulnerabilities and exposures. The same will be true for storage, network, and end-point components. People,  process, and third-party vulnerabilities can be determined by similar  methodologies.

Of note, vulnerabilities and (effective) controls exist in a kind of  reverse symbiosis: where one is present the other is not. Where  sufficient control is present, the vulnerability is neutralized; without the control, the vulnerability persists. Thus, the enterprise’s  vulnerabilities are most practically organized according to the  enterprise-approved control framework.    2  Here synergies begin to emerge. Using a common framework and language,  the security, risk, IT, and frontline teams can work together to   identify what needs to be done to close vulnerabilities, guide  implementation, and report on improvements in exactly the same manner  and language. Experience confirms that when the entire organization  shares a common way of thinking about vulnerabilities, security can be  significantly enhanced.

**4. Understand relevant threat actors and their capabilities**

The groups or individuals an organization must worry about—the threat actors—are determined by how well that organization’s assets fit with  the attackers’ goals—economic, political, or otherwise. Threat actors  and their capabilities—the tactics, techniques, and procedures they use  to exploit enterprise security—define the organization’s threat  landscape.

Only by understanding its specific threat landscape can an  organization reduce risk. Controls are implemented according to the most significant threats. Threat analysis begins with the question, Which  threat actors are trying to harm the organization and what are they  capable of? In response, organizations can visualize the vulnerabilities commonly exploited by relevant threats, and appropriate controls can  then be selected and applied to mitigate these specific vulnerability  areas.

In identifying the controls needed to close specific gaps,  organizations need to size up potential attackers, their capabilities,  and their intentions—the threat actors’ strength and will (intention) to create a risk event. This involves collecting information on and  understanding how the attackers connect, technically and nontechnically, to the people, process, and technology vulnerabilities within the  enterprise.

**5. Address vulnerabilities**

To defeat threat actors, vulnerabilities discovered in the third  action we describe will either be closed by existing controls—normal run activities or existing change initiatives—or will require new control  efforts. For existing controls, the cyber governance team (for “run”)  and the program management team (for “change”) map their current  activities to the same control framework used to categorize  vulnerabilities. This will show the controls already in place and those  in development. Any new controls needed are added to the program backlog as either stand-alone or composite initiatives.

While an organization may not be able to complete all initiatives in  the backlog in a single year, it will now be able to choose what to  implement from the full spectrum of necessary controls relevant to the  enterprise because they are applicable for frustrating relevant threat  capabilities. The risk-based approach importantly bases the scope of  both existing and new initiatives in the same control framework. This  enables an additional level of alignment among teams: delivery teams  charged with pushing and reporting on initiative progress can finally  work efficiently with the second and third lines of defense (where  relevant), which independently challenge control effectiveness and  compliance. When the program-delivery team (acting as the first line of  defense) sits down with the second and third lines, they will all be  speaking the same language and using the same frameworks. This means  that the combined groups can discuss what is and is not working, and  what should be done.

**6. Map the enterprise-risk ecosystem**

A map of enterprise risks—from the enterprise-risk-management  framework to enterprise vulnerabilities and controls to threat actors  and their capabilities—makes visible a “golden thread,” from control  implementation to enterprise-risk reduction. Here the risk-based  approach can begin to take shape, improving both efficiency in the  application of controls and the effectiveness of those controls in  reducing risks.

Having completed actions one through five, the organization is now in a position to build the risk-based cybersecurity model. The analysis  proceeds by matching controls to the vulnerabilities they close, the  threats they defeat, and the value-creating processes they protect. The  run and change programs can now be optimized according to the current  threat landscape, present vulnerabilities, and existing program of  controls. Optimization here means obtaining the greatest amount of risk  reduction for a given level of spending. A desired level of risk can be  “priced” according to the initiatives needed to achieve it, or the entry point for analysis can be a fixed budget, which is then structured to  achieve the greatest reduction in risk.

Cybersecurity optimization determines the right level and allocation  of spending. Enterprise-risk reduction is directly linked to existing  initiatives and the initiation of new ones. The analysis develops the  fact base needed for tactical discussions on overly controlled areas  whence the organization might pull back as well as areas where better  control for value is needed.

By incorporating all components in a model and using the sources of  value and control frameworks as a common language, the business, IT,  risk, and cybersecurity groups can align. Discussions are  framed by  applying the enterprise control framework to the highest sources of  value. This creates the golden-thread effect. Enterprise leadership  (such as the board and the risk function) can identify an enterprise  risk (such as data leakage), and the cybersecurity team can report on  what is being done about it (such as a data-loss prevention control on  technology or a social-engineering control on a specific team). Each  part is connected to the other, and every stakeholder along the way can  connect to the conversation. The methodology and model is at the center, acting both as a translator and as an optimizer. The entire enterprise  team knows what to do, from the board to the front line, and can move in a unified way to do it.

**7. Plot risks against risk appetite; report on risk reduction**

Once the organization has established a clear understanding of and  approach to managing cyberrisk, it can ensure that these concepts are  easily visualized and communicated to all stakeholders. This is done  through a risk grid, where the application of controls is sized to the  potential level of risk (Exhibit 4).

      Exhibit 4                                                                                            We strive to provide individuals with  disabilities equal access to our website. If you would like information  about this content we will be happy to work with you. Please email us  at: [McKinsey\_Website\_Accessibility@mckinsey.com](mailto:McKinsey_Website_Accessibility@mckinsey.com)

The assumption in this use of the classic risk grid is that the  enterprise-risk appetite has been defined for each enterprise risk. The  potential impact for each enterprise-risk scenario can then be plotted  on the risk grid. Once the relationships among the threats,  vulnerabilities, and applied controls are modeled and understood, the  risks can be evaluated according to their likelihood. As more controls  are applied, the risk levels are reduced to the risk appetite. This is  the way the cyber program can demonstrate impact in terms of  enterprise-risk reduction.

As new threats emerge, new vulnerabilities will become apparent.  Existing controls may become ineffective, and enterprise risks can move  in the opposite direction—even to the point where risk-appetite limits  are exceeded. For information-security-management systems, the risk grid allows stakeholders to visualize the dynamic relationships among risks, threats, vulnerabilities, and controls and react strategically,  reducing enterprise risks to the appropriate risk-appetite level.

**8. Monitor risks and cyber efforts using risk appetite and key cyberrisk and performance indicators**

At this point, the organization’s enterprise risk posture and threat  landscape are understood, and the risk-based cybersecurity program is in place. The final step is to monitor and manage for success.

Many companies attempt to measure cyber maturity according to program completion, rather than by actual reduction of risk. If a security  function reports that the data-loss-prevention (DLP) program is 30  percent delivered, for example, the enterprise assumption is that risk  of data leakage is 30 percent reduced. If a multifactor authentication  initiative is 90 percent implemented, the assumption is that the risk of unauthorized access is almost eliminated. These assumptions are false,  however, because actual risk-reducing results are not being measured in  these examples.

Metrics need to measure both inputs and outputs; inputs in this case  are risk-reduction efforts undertaken by the enterprise, while the  output is the actual reduction in enterprise risk. The input metric here is a key performance indicator (KPI): measuring the performance of a  program or a “run” function. The output metric is really a key risk  indicator (KRI), measuring the risk level associated with a potential  risk scenario.  The thresholds for the KRIs must be tied directly to  risk-appetite levels (the KPI thresholds can also be linked in this  way). For example, if risk appetite for data leakage is zero, then the  systemic controls (and corresponding “red” thresholds) must be higher  than they would be if a certain percentage of leakage is allowed over a  certain period. Of course, tolerances for cyber incidents may be not  always be set at zero. In most cases, it is impossible to stop all cyber attacks, so sometimes controls can be developed that tolerate some  incidents.

One way to think about KRIs and KPIs is with regard to the  relationship between altitude and trajectory. A KRI gives the current  risk level of the enterprise (the “risk altitude”) while the KPI  indicates the direction toward or away from the enterprise-risk-appetite level (“risk trajectory”). An enterprise may not yet have arrived at  the leadership’s KRI target but a strong KPI trajectory would suggest  that it will soon. Conversely, an enterprise may have hit the desired  KRI threshold, but the KPIs of the run activity may be backsliding and  give cause for concern.

Executives are often forced to make sense of a long list of sometimes conflicting metrics. By linking KRIs and KPIs, the cybersecurity team  gives executives the ability to engage in meaningful problem-solving  discussions on which risks are within tolerances, which are not, and why (see the sidebar, “Linking a KRI to a KPI”).

The [risk-based approach to cybersecurity](https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-linchpin-of-the-digital-enterprise) is thus ultimately interactive—a dynamic tool to support strategic  decision making. Focused on business value, utilizing a common language  among the interested parties, and directly linking enterprise risks to  controls, the approach helps translate executive decisions about risk  reduction into control implementation. The power of the risk-based  approach to optimize for risk reduction at any level of investment is  enhanced by its flexibility, as it can adjust to an evolving  risk-appetite strategy as needed.

Many leading companies have a cyber-maturity assessment somewhere in  their archives; some still execute their programs to achieve certain  levels of maturity. The most sophisticated companies are, however,  moving away from the maturity-based cybersecurity model in favor of the  risk-based approach. This is because the new approach allows them to  apply the right level of control to the relevant areas of potential  risk. For senior leaders, boards, and regulators, this means more  economical and effective enterprise-risk management.