The seven ways of the agile CISO

Cyber security leadership in the age of fast and continuous delivery

KPMG International

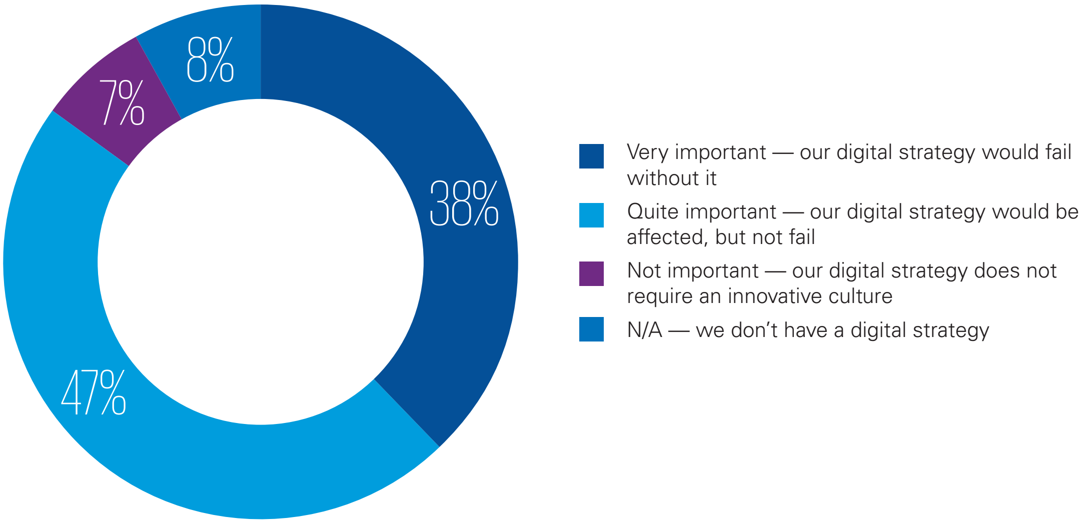
home.kpmg

Resistance is futile (change is inevitable?)

As digital transformation dramatically disrupts and redefines the business landscape with unprecedented speed, today’s forward-looking business leaders are recognizing the inevitable need to experiment with new technologies and ideas, test the market and respond quickly with timely innovations.

In the 2018 CIO Survey by KPMG and Harvey Nash, global technology executives indicated the need for an “innovative, experimental culture” to support a digital strategy designed for success.

How important is it to have an innovative, experimental culture in your organization to ensure its digital strategy is a success?



Source: Harvey Nash/KPMG CIO Survey 2018 — The transformational CIO, KPMG International, 2018.

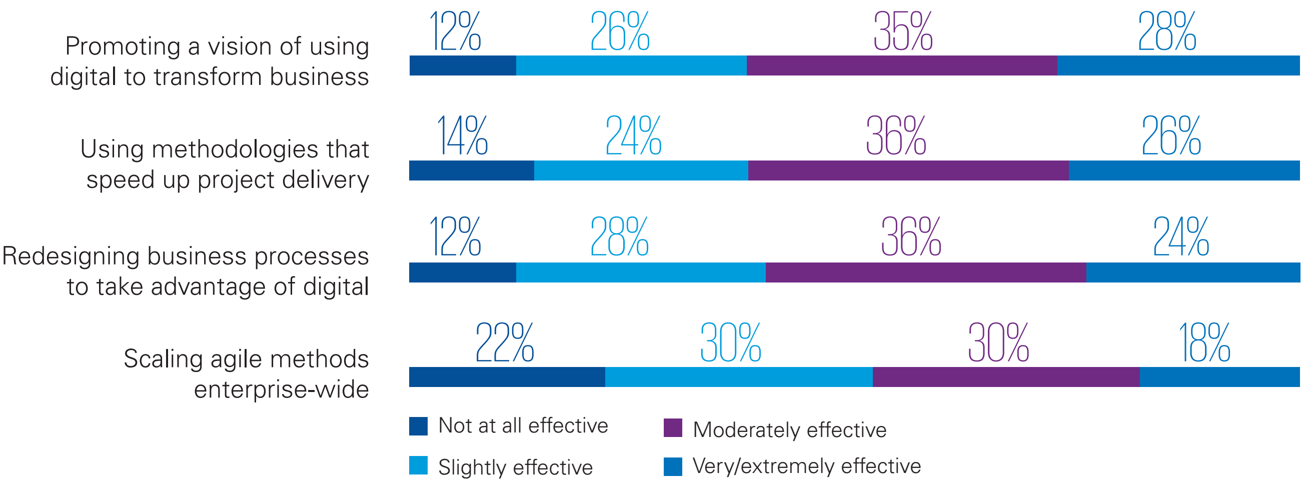
However, experimentation and innovation typically do not come easily to most organizations and this perhaps has never been truer than in today’s world of rapid and dramatic change. Experimentation requires the ability to:

- quickly turn ideas into working prototypes
- take them to production environments
- test them with consumers
- quickly evolve prototypes into agile products.

Under this premise, traditional product delivery methods typically fall short for organizations that are transforming their technology operating models in order to speed up their delivery capabilities.

Despite being simple in nature, ‘agile methodologies’ — and related materializations (DevOps, Lean, etc.) — designed to accelerate production and the frequency of product releases can pose significant challenges to organizations. As noted in the 2018 CIO Survey by Harvey Nash and KPMG, adopting more agile methods designed to accelerate product delivery to the market is identified as a key challenge by most Chief Information Officers (CIOs).

How effective is your organization in the following capabilities?



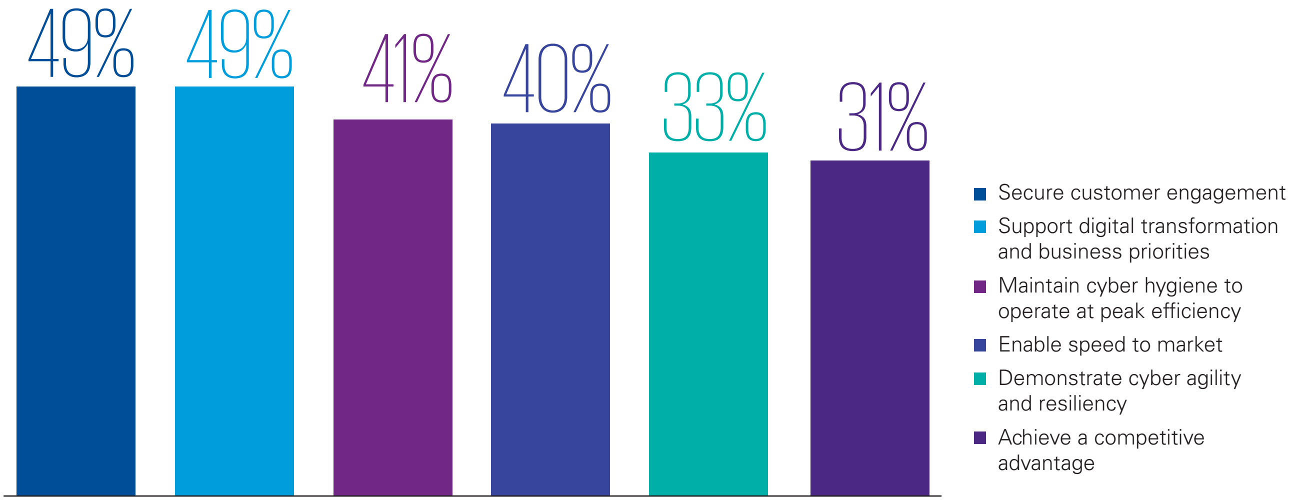
Source: Harvey Nash/KPMG CIO Survey 2018 — The transformational CIO, KPMG International, 2018.

One of the most significant challenges to achieving an agile-based approach is cyber security. Why? Because having the speed and agility to experiment efficiently and deliver products more quickly to generate competitive advantages is of little value if it heightens an organization's cyber security risk. A cyber breach can destroy or severely undermine customer confidence and brand reputation in an instant. As most approaches to securing software is designed from a 'gated' perspective in which specific security controls are embedded in a product stage lifecycle, the agile journey raises the question of choosing software security that's designed to optimize transformation and continuous flow.

Based on the results of KPMG's Consumer Loss Barometer — The economics of trust, security executives see themselves as an integral part of digital transformation, with agility and customer protection among the top topics cited.

Simultaneously addressing the need for agile methods and the need to sustain adequate cyber security presents certain challenges for the Chief Information Security Officer (CISO) navigating a transforming business landscape. In this article we will provide timely insights on how best to 'go fast safely.' We will examine both the challenges organizations are grappling with today and a strategic framework designed to help CISOs successfully complete this journey by significantly minimizing friction, delivering value more quickly and, ultimately, enhancing competitiveness via more frequent product releases.

We asked respondents how cybersecurity could enable growth:



Source: Consumer Loss Barometer — The economics of trust. KPMG International, 2019.

The new CISO: Evolving from gatekeeper to bodyguard

> “While top executive engagement on cyber security has been growing, our Consumer Loss Barometer — The economics of trust survey found that the majority of CEOs still have very scarce involvement with cyber themes.”

In addition to optimizing processes and performance in ways that enhance competitiveness, smart digital leaders recognize cyber security as a critical feature of their digital journey. And driving cyber security innovation aimed at future growth and success must be managed initially by the CEO and CISO.

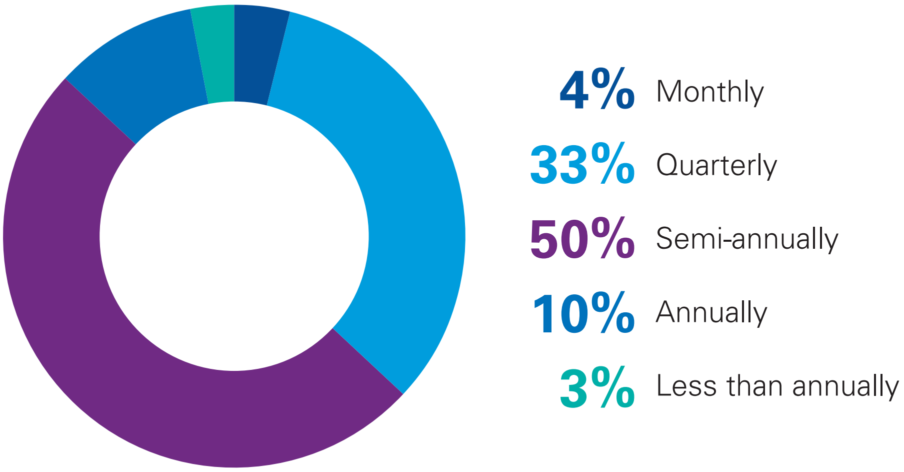
Strategic, future-focused CEOs need to articulate a clear and well educated message to fellow business leaders, boards and employees on the critical role of cyber security as an inevitable starting point for successful transformation. This also implies a new level of commitment from leadership to be fully educated on today's complex security challenges and digital opportunities. While top executive engagement on cyber security has been growing, our Consumer Loss Barometer — The economics of trust survey found that the majority of CEOs still have very scarce involvement with cyber themes.

The CISO, meanwhile, must evolve their role from traditional gatekeeper to the CIO's trusted bodyguard — playing a significantly expanded and strategic collaborative role aimed at ensuring that the CIO and teams feel comfortable providing the CISO with open feedback and insights. This requires a commitment from the CISO to:

- educate and implement new software development paradigms
- challenge traditional thinking to unlock greater experimentation and innovation and enhanced speed to market
- advance a new type of conversation with the CIO that includes a focus on greater ongoing collaboration that aims to accelerate production and generate new advantages in the market.

A critical stage in this initial organizational transformation is fostering ongoing dialogue between the CISO and CIO as they work together to build an agile and resilient organization. As a recent State of DevOps Report noted, transformational leadership is a key component to success for modern software delivery programs.

Sizeable minority say executives infrequently briefed on cyber security



Source: Consumer Loss Barometer — The economics of trust. KPMG International, 2019.

Fifty-one percent of security executives report they have little or no input into the digital transformation agenda. From KPMG's research on the Consumer Loss Barometer — The economics of trust, we find that while cyber security executives appreciate the potential for cyber to add value to their business growth agenda, their teams are not yet consistently embedded within their digital transformation agenda. To achieve that, cyber security capabilities need to match the agility of the digital organization, adapting to meet the fast-changing needs of stakeholders with the right mandate to enable digital transformation.

Challenges — and opportunities — for CISOs in the age of continuous delivery

Having established a platform for deeper collaboration between the CISO and CIO, it's crucial for the CISO to review the organization's processes and promote their proactive 'bodyguard' role within the business. Outlined below are the key triggers and challenges faced by CISOs:

1 An agile delivery model requires more continuous participation by cyber security leaders

In a Gantt chart based project, cyber security usually has predefined contact points within the team's detailed planning and work schedule. These typically occur during initial software architecture definition and validation, with a couple of checkpoints ending with late testing and acceptance of the solution. If the application was particularly sensitive, annual testing may be required as well.

Today, modern application security replaces the typically predefined 'few and heavy' periodic interactions in the software lifecycle with more frequent and lighter, or smaller, interactions that increase dialogue, collaboration and efficiency while expediting the entire development process. For example, security specialists are embedded early in the planning and design of an application, automated security testing takes place prior to merging code (and after deployment), and pen tests may be replaced by bug bounty programs to identify issues and vulnerabilities as quickly as possible.

While the organic way to embrace this continuous approach would be to embed cyber professionals within agile teams, most cyber security departments are typically not staffed to support this approach.

This poses the first challenge — how to re-organize cyber security to support this interaction, either through staffing, automation or clever methodological work-arounds (i.e. identify and participate as needed in cyber-intensive sprints that focus specifically on innovations or necessary changes related to cyber security during development).

2 An agile friendly cyber department needs to increase its understanding of modern software development dynamics and techniques

Traditionally, cyber security and software development professionals came from different backgrounds and career paths. Take a sample of your cyber security team and chances are they come from:

- a pure cyber security background — they started their career in this field
- an IT audit/risk management background — they started as IT auditors and moved to cyber security
- an infrastructure/networking background — they started as administrators or related roles that incrementally moved to cyber security.

These professionals typically work beyond the realm of actual software development. The typical cyber professional not only has some distance from the intricacies of development, but most likely interacts with coders in a more traditional control oriented, gated dynamic. The initial reaction of cyber security professionals may be to view this approach as too light — a similar initial reaction to agile methods. But this response is the opposite of what is needed in a modern cyber security department.

This dynamic poses the second crucial challenge — how to incorporate this modern development understanding into the cyber security team. It's not rare today to see cyber departments hiring software developers possessing a strong understanding of modern dynamics and training them in cyber security. Some digital native organizations are going even further by hiring CISOs with a development background or promoting CISOs from their development ranks.

3 Cyber friendly software development is needed for effective cyber security to flourish

Software development teams need to incorporate cyber security throughout their organizational structure and strategic initiatives. It's similarly important for development teams and cyber security professionals to bridge the gap between them — ensuring siloes are broken down and collaboration is at the center of everything they do. Development and cyber security players seeking success and enhanced competitiveness therefore need to see themselves as part of the same team pursuing a common goal.

This third challenge involves raising the status of security within developers' priorities.

4 Autonomous development teams and high automation may pose a segregation-of-duties challenge if not properly designed

In a siloed, stage-gate process — in which each software development stage is separated by a so called 'gate' requiring approvals before development moves to the next stage — segregation of duties (SOD) is easy: those who develop do not certify production readiness and those who deploy do not develop. Unfortunately, this strict separation of duties frequently creates prioritization and agenda conflicts between siloed development teams and security professionals.

Overcoming this conflict requires changing the way we think of SOD, from segregating duties to *segregating automation of duties*. A fully automated delivery pipeline may allow developers to release code upon check-in, but would still force developers to go through strict acceptance tests, security tests and other pre-deployment checks. Where is SOD in this automation intensive scenario? Acceptance tests are developed by the QA department and development has no influence over them; deployment scripts are developed by operations and development cannot modify them; security checks are developed by the cyber security department, and so on.

This poses a fourth challenge to the organization. On one hand, departments involved in the software lifecycle must incorporate automation capabilities. On the other, audit and compliance leaders must be educated to understand how their control goals can be met through automation, and how the controls themselves must be revamped to facilitate automation. And finally, new controls — such as a production automation that engineer's independence from development engineers — must be implemented.

5 Continuous, rapid delivery may require tradeoffs

A key capability in delivering software successfully is reducing batch size so that new releases happen more often. This enables the business to deliver value in smaller regular increments. Leaders can quickly learn whether new software features resonate with users or require pivoting to alternate opportunities.

To meet the fast pace of delivery in environments deploying multiple times per day, it may be necessary to apply only a subset of the available automated security tests. For example, if a security scanner takes 12 hours to run all tests, leaders may agree to test only for highest-risk vulnerabilities and defer the rest to a weekly cycle. This compromise enables rapid delivery of new features while significantly mitigating risk.

Similarly, while the likelihood of software bugs or vulnerabilities in a given release is reduced via modern application security approaches, the possibility of an issue making its way into software in production will always remain. This therefore requires the ability to quickly rollback to a 'known good' state that may be achievable without a redeploy.

Fortunately, as teams learn to deliver quickly, pushing another recent version into production is less daunting than relying on infrequent releases. This practice may be one of the most underappreciated advantages of agile and DevOps approaches.

A fifth challenge for organizations is the level of acceptable production risk allowed in favor of a faster release. Doing so may look risk friendly from a traditional perspective but poses both a technical and organizational challenge to the modern cyber organization.

6 Increasing cloud usage poses a moving security target

A pure DevOps organization will tend to make heavy use of cloud capabilities, creating a 'moving target' in terms of security infrastructure. As applications scale up or down to meet user demand, the lifespan of infrastructure may be significantly shorter than that of traditional hosts in a data center. Leaders and risk management teams must acknowledge that classes of infrastructure may be ephemeral and traditional security approaches may no longer work.

A sixth challenge involves pressure on today's infrastructure teams to deploy secure images prior to production. However, server-free architectures changes the risk equation away from traditional approaches. When there are no hosts to manage, patch or scan for vulnerabilities, responsibility for managing the environment is transferred to the cloud provider. The challenge here is that the cost can be higher than traditional virtual hosts, creating a different class of organizational risk.

The seven ways of the agile CISO

Like it or not, resistance is futile — and dramatic change is inevitable — for organizations pursuing heightened future competitiveness and sustained success. Most organizations will need to adopt agile and continuous delivery practices in important systems, ensuring CISOs overcome the significant challenges outlined above. Cyber security leaders will likely find that some agile or continuous delivery practices are already being used in small pockets of the organization.

Here are the seven recommended ways for CISOs to reinvent themselves and their cyber organization in the era of continuous delivery.

1 Flow — the need for continuous participation versus discrete control points

With the acceleration of development practices, security teams must adopt strategies that meet increased throughput. Security should provide flexibility that empowers developers to focus on product delivery without compromising acceptable organizational risk. This can be achieved in the following ways:

- **Create a delivery support team with the cyber security department.** Development teams and cyber security teams must be aligned to better understand 'cyber-intensive sprints' — cyber security focused interactions involving the cyber security team's participation at specific stages of the software/application development process.
- **Develop standards and best practices** to embed security in application development without requiring continuous participation from security. A set of predefined, cyber approved design decisions, including coding standards, design patterns and more can significantly enhance processes and efficiency.
- **Allow self-service as much as possible.** To start with, identify and configure automated review tools and provide them to development to assess their solutions. A security testing sandbox can be provided for solutions that can be deployed and automatically tested without security interference. Security teams should ensure that these platforms can handle rising demand.
- **Incorporate cyber security team members into initial project design stages.** This allows security needs to be considered from project inception and avoids later modifications that cost time and money.

2 Secure development evangelism — the need for security skills on construction teams

Although organizations can implement any number of new tools or processes, a strong change-management system is crucial to ensuring successful adoption. This can be achieved in the following ways:

- **Create a consistent security champion program** as a touch point between developers and security. This will give developers a significant and effective stake in product security throughout the development process.
- **Drive consistent messaging** from your executive leadership throughout the organization, with a focus and commitment to security improvements.
- **Tailor your security training.** Take the time to develop interactive and collaborative training programs that are relevant to your workforce, that empower your development teams and that deliver effective, goal-oriented solutions for your organization.

3 Delivery mindset — educating cyber security teams on agile principles

Just as it is crucial to promote the importance of security organization-wide, the security team must also understand the full impact of an agile approach. The security function must integrate itself as a vital partner to the organization and its diverse teams. This can be achieved in the following ways:

- **Communicate the importance of partnering** with teams across functions. Promoting strong partnership and collaboration between security and development can dramatically enhance efficiency, results and competitiveness.

- **Support the education of security team members** on modern delivery models. An understanding of the specific tools used by various contributing functional groups will provide a thorough problem solving knowledge base for security use cases and a deeper understanding of development challenges.
- **Inform your team about a shift in security strategy.** Security must understand the concept of acceptable risk and how that impacts their day-to-day operations.

4 Cyber automation — the need for control automation

In order to accelerate security as agile methods emerge, investment in strategic automation must be implemented across the software delivery life cycle (SDLC) to ensure the longevity of security programs within the organization. This can be achieved in the following ways:

- **Automate smarter.** Strategically identifying which areas to automate in your organization will ensure greater ROI, stronger security automation decisions and reduced risk.
- **Begin with a small amount of security scrutiny** that can be automated in a tool and turn up the volume slowly once developer and operations teams have adjusted to the new processes with remediation tickets.
- **Avoid false positive findings.** Ensure that the work your automated tools create for the operation and developer teams requires their attention.
- **Integrate cyber security automation with automation efforts** of other teams to maximize overall efficiency and results via closer ongoing collaboration. If the team has a continuous integration/continuous delivery (CI/CD) pipeline tool in place for deployments, build security tests that integrate directly with it.

5 Cyber telemetry — the need for cyber security insight along the software lifecycle

The modern digital business is driven by data. There is an opportunity for security systems within the organization to utilize appropriate telemetry and feedback tools where possible. Proper use allows security to put risk reduction into a tangible report while also examining the effectiveness of various security controls across the organization.

- **Create templates of code** that can be copied and pasted into development projects providing the telemetry desired by the security team. This eliminates any excuse from development that there is not enough time for them to meet the custom demands from security and it provides standard metrics to compare across products and applications.
- **Examine how increased telemetry can help** the development team meet goals. As organizations become more focused on security, development teams have more responsibility to meet security standards. Telemetry that displays the results of their work will be seen as a positive for development teams making the extra effort to secure their product.
- **Turn it on when you can.** If you purchase a next generation Static Application Security Testing tool, use its telemetry capabilities to analyze its effectiveness. This will show the software development team that you are paying attention to the false positive test results they are receiving and are supporting the partnership.

6 Cyber-debt management — the responsible management of cyber security trade-offs

IT and development must manage technical debt, which is a result of choosing a quickly implemented solution that costs more in the long term versus choosing the right sustainable solution which may be more of an expensive investment up front. The implied cost/tradeoff of choosing a limited but more rapid solution (or technical attributes) instead of an enhanced solution requires more time and cost. Security teams should also manage 'cyber debt' that can be accumulated in an agile organization. Similar to the concept of technical debt, cyber debt involves the implied costs and tradeoffs of delivering cyber security features today that speed up development but at the expense of potential security enhancements. This can be managed in the following ways:

- **Start small with security initiatives.** If successful, expand to other teams to grow naturally across iterations, and assist the team to more accurately focus on pain points.
- **Review the progress of security initiatives frequently.** Large-scale security investments can be extremely costly, so ensure consistent monitoring throughout the production journey.
- **Prioritize your resources.** When you can demonstrate the value your team is providing, it becomes easier to request additional budget and resources. This ties back to starting small — many organizations credit the effectiveness of their security program to prioritization. Identify where the greatest risk exists and start there.
- **Lower existing cyber debt.** Figure out a process that gives your team time to improve on the cyber debt that exists across the organization so that it never rises to unmanageable levels.

7 Expanded vision — securing an expanding infrastructure

Just as security must adapt to the speed of product delivery, it must also adapt to the increased scope of technologies used in faster delivery. Containers, cloud hosts, virtual machines — all come with their own set of security considerations that seem to increase the workload for security. Securing an expanding infrastructure can be achieved in the following ways:

- **Embrace technologies used by the organization.** Technology will continue to evolve and security will never be the final say in determining the internal tools other teams can or cannot use. But if security integrates with the toolset used throughout the organization, this can improve the overall security posture by simplifying the responsibilities of others. Cyber security teams should also be very strategic and forward focused on automating security controls in an ever-evolving tech environment.
- **Leverage the ability to replicate** modern infrastructure tools for security benefits. The use of infrastructure as code allows security to have a very tangible understanding of deployments that exist throughout the enterprise. If security then adds their own considerations into those deployment scripts, it can ensure infrastructure meets their requirements regardless of how many hosts are being spun up each day. While collaboration is key, security must ensure that their requirements are included and have control mechanisms to guarantee security considerations before any live deployment.

Preparing for the journey ahead

Transforming to an agile organization poses significant challenges and opportunities for any CISO. The focus on speed can often appear to disregard existing security programs. At the same time, cyber security is a priority for today's savvy consumers and CISOs are thus facing increased scrutiny from business leaders and boards to optimize security for today and tomorrow.

Organizational changes toward agile methodologies have much to offer but need to include appropriate innovation that impacts people, processes and technology along the way — no simple task for any organization.

But the agile CISO will have a diverse toolkit to rely on. Depending on your organization's environment and objectives, different methods will be more effective than others in completing the journey. As the CISO, consider it your job to understand all options that exist in the journey to transform legacy, siloed and slow IT operating models into integrated business-driven engines that power agility, drive performance and manage risk. Future competitiveness in the digital age will demand nothing less. As CISOs prepare for this journey, here are a few questions for cyber security executives to reflect on:

- Does my team possess the appropriate skills to promote and sustain a more-innovative, experimental and collaborative culture?
- Does my strategy going forward promote increased collaboration at every step to ensure organization-wide alignment of goals and evolving capabilities?
- What is our current understanding of agile operating models and development methods?
- Am I having conversations with peers (CTO, CIO) about more agile methodologies and how closely aligned KPIs and objectives are across the various departments?
- Am I having informed and ongoing conversations with C-Suite leaders on the role of cyber security within innovation?

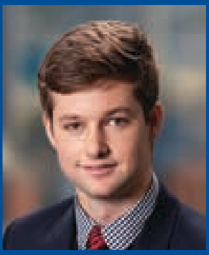
How can we help?

KPMG's Cyber Security services assists global organizations in transforming their security, privacy, and continuity controls into business enabling platforms while maintaining the confidentiality, integrity and availability of critical business functions. The KPMG Cyber Security approach strategically aligns with clients' business priorities and compliance needs.

Contributors

Walter Risi
Partner, Cyber Security
KPMG in Argentina
E: wrisi@kpmg.com.ar

Caleb Queern
Director, Cyber Security
KPMG in the US
E: cqueern@kpmg.com



Kyle McNulty
Associate, Cyber Security
KPMG in the US
E: kylemcnulty1@kpmg.com

Contact us

Akhilesh Tuteja
Global Cyber Co-Leader
KPMG International
E: atuteja@kpmg.com

Tony Buffomante
Global Cyber Co-Leader
KPMG International
E: abuffomante@kpmg.com

The Americas

Greg Bell
Chief Technology Officer, Advisory
KPMG in the US
E: rgregbell@kpmg.com

Francois Beaudoin
Cyber Security Leader
KPMG in Canada
E: fbeaudoin@kpmg.ca

Leandro Antonio
Americas Cyber Security Leader
KPMG in Brazil
E: lantonio@kpmg.com.br

Europe

Luca Boselli
Cyber Security Leader
KPMG in Italy
E: lboselli@kpmg.it

John Hermans
EMA Cyber Security Leader
KPMG in the Netherlands
E: hermans.john@kpmg.nl

Mika Laaksonen
Cyber Security Leader
KPMG in Finland
E: mika.laaksonen@kpmg.fi

Matthias Bossardt
Cyber Security Leader
KPMG in Switzerland
E: mbossardt@kpmg.com

Martin Tyley
Cyber Security Leader
KPMG in the UK
E: martin.tyley@kpmg.co.uk

Vincent Maret
Cyber Security Leader
KPMG in France
E: vmaret@kpmg.fr

Uwe Bernd-Striebeck
Cyber Security Leader
KPMG in Germany
E: uberndstriebeck@kpmg.com

Marc Martinez
Cyber Security Leader
KPMG in Spain
E: marcmartinez@kpmg.es

Asia Pacific

Matthew O'Keefe
ASPAC Cyber Security Leader
KPMG in Australia
E: mokeefe@kpmg.com.au

Gordon Archibald
Cyber Security Leader
KPMG in Australia
E: garchibald@kpmg.com.au

Daryl Pereira
Cyber Security Leader
KPMG in Singapore
E: darylpereira@kpmg.com.sg

Henry Shek
Cyber Security Leader
KPMG in China
E: henry.shek@kpmg.com

Atsushi Taguchi
Cyber Security Leader
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

Atul Gupta
Cyber Security Leader
KPMG in India
E: atulgupta@kpmg.com

Shaked Levy
Cyber Security Leader
KPMG in Israel
E: shakedlevy@KPMG.com

home.kpmg/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by Evalueserve.

Publication name: The seven ways of the agile CISO

Publication number: 136283-G

Publication date: June 2019