Perspectives

Grant Waterfall: Take a two-sided approach to cybersecurity and privacy for long-term success

April 2016

pwc

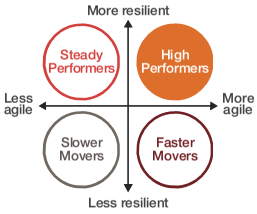
This year's Risk in review study[1] focuses on two critical components of risk management. The first is **risk resiliency**—the ability to withstand business disruption by relying on solid processes, controls and risk management tools and techniques, including a well-defined corporate culture and a powerful brand. The second is **risk agility**—the ability to alter and adapt risk management infrastructure to respond quickly to changing market dynamics or customer preferences.

These twin concepts take special meaning in the context of cybersecurity and privacy. In this sense, risk resiliency means investing in a broad-based cybersecurity risk management program that automates security and privacy controls and minimizes system downtime in the event of an attack. Risk agility, meanwhile, is about pivoting security attention to support the rapid development of customer-facing digital technology that drives revenue, and using advanced analytics and monitoring techniques to better predict, detect and respond to a rapidly changing digital and threat landscape.

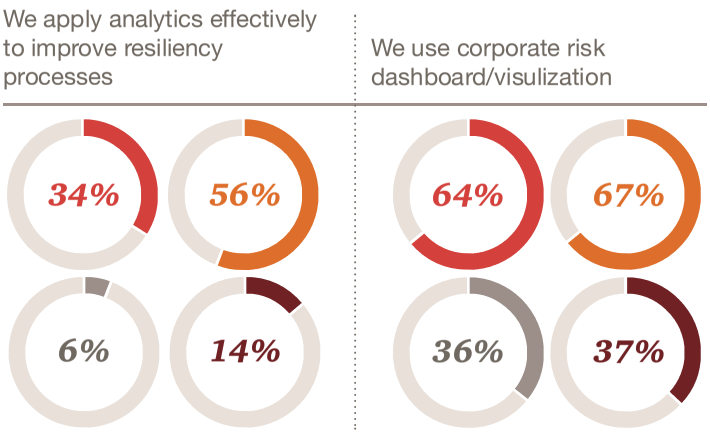
We believe companies need to think broadly but move boldly[2] when it comes to cybersecurity and privacy. Risk resiliency is about strength and thinking broadly: it fortifies your company's systems, data, and intellectual property, helping to defend your company from harm. In contrast, risk agility is about speed, so companies can move boldly: In a digital world, companies are racing to create new customer-facing applications and tools to drive new revenue, from electronic wallets to contextual advertising to wearable devices. Is your company's cybersecurity team doing enough to support that rapid development? Risk agility means that cybersecurity professionals are helping get those new technology deployments to customers sooner by clearing the path of security and privacy roadblocks. And that's a huge opportunity.

Figure 1

Faster Movers do not apply analytics as effectively as High Performers



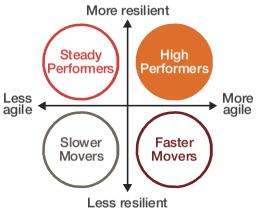
Respondents report:



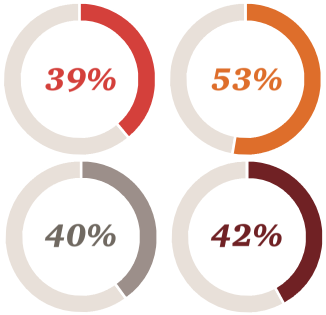
Source: PwC's Risk in review 2016: Going the distance
pwc.com/riskinreview

Figure 2

High Performers have well-defined and automated IT security processes



Respondents who report they have well-defined and automated IT security processes:



Source: PwC's Risk in review 2016: Going the distance
pwc.com/riskinreview

But our report points to some important trends. Our study's Faster Movers[3]—companies that are highly risk-agile but not highly risk-resilient—are moving quickly to identify and pursue new opportunities ahead of competitors, diversity their portfolio and transform their technology platforms. They are also more likely than other respondents to expect significant revenue and profit-margin growth (of greater than 5%). But they are less likely to leverage data analytics to assist them in their decision-making, monitor Key Risk Indicators (KRIs), or use tools like dashboards and visualizations. This can seriously weaken their security, and hamper their ability to move quickly and effectively as they attempt to launch new products or enter new markets. In contrast, High Performers (companies that are both risk-resilient and risk-agile) are far more likely to leverage these capabilities—and are only slightly less likely than Faster Movers to expect significant growth.

[1] See PwC's full Risk in review 2016 study at pwc.com/riskinreview

[2] See PwC's Global State of Information Security 2016 report

[3] Please see page 3 for additional context on companies identified as High Performers and Faster Movers in PwC's Risk in review 2016 study

The important connection between risk resiliency and risk agility

Our analysis shows that risk-agile companies are more likely to expect significant revenue and profit-margin growth than those that are not risk agile. But agility takes you only so far: companies we've termed Faster Movers pursue risk agility at the expense of risk resiliency; they may lack strategies for business continuity, succession planning, strategic alignment, and data analytics—all of which are critical for enduring success.

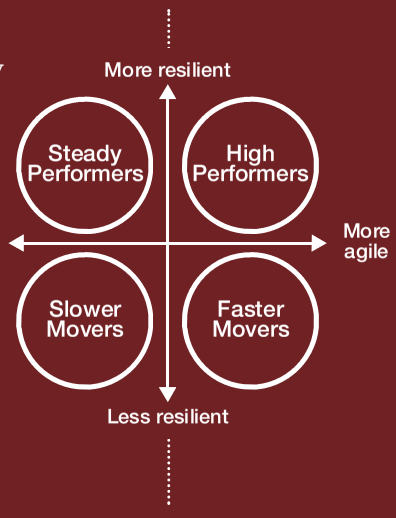
In sharp contrast, High Performers—the 36% of survey respondents who are both highly risk agile and highly risk resilient—establish strong risk management cultures and structures that ensure their ability to weather risk events, which in turn allows them to quickly and confidently respond to changes in their risk profiles. Remarkably, High Performers are even more risk agile in almost every measure than Faster Movers. And the real kicker: they are only slightly less likely to expect significant growth (i.e. greater than 5%). In other words, they've taken advantage of their risk management organization and strategies to find the sweet spot at the intersection of strong growth and sustainable success.

Performers and movers: Building the risk resiliency/risk agility matrix

In our survey, we asked companies questions about their risk-resiliency and risk-agility capabilities, processes, and corporate characteristics. We then scored their answers on a 0–100 scale to create a risk resiliency/agility matrix. Respondents fell into four quadrants.

Steady Performers
Companies scoring high on resiliency but lower in agility.

High Performers
Companies in the sweet spot of being both highly risk agile and highly risk resilient



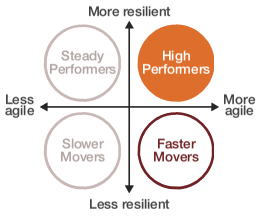
Slower Movers
Companies scoring low on resiliency and low on resiliency

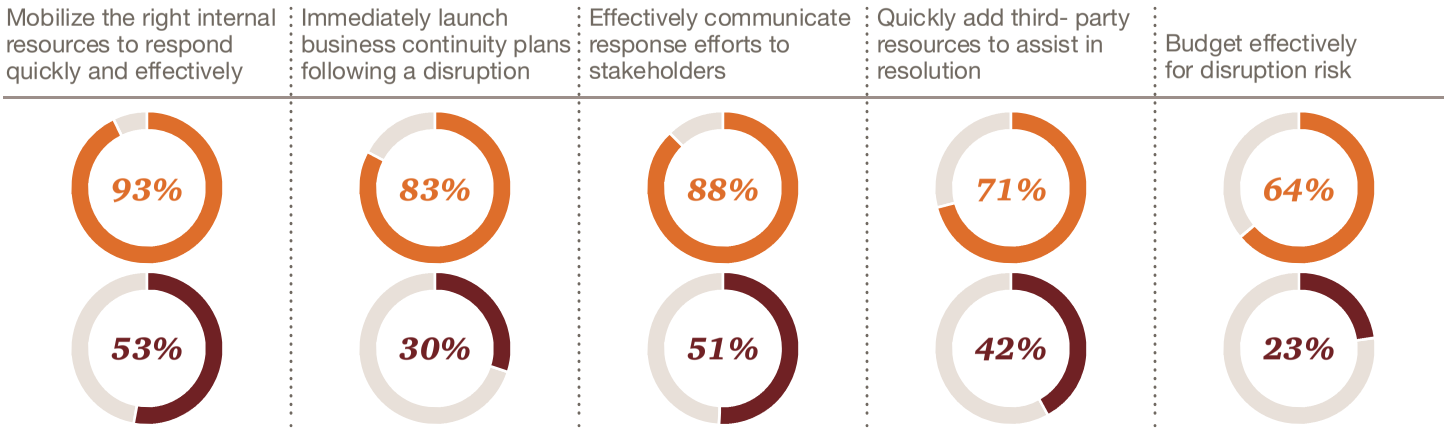
Faster Movers
Companies which are highly agile but not highly resilient

Figure 3

Faster Movers need to improve business continuity strategies

High Performers and Faster Movers report their companies have the following business continuity strategies in place:





Source: PwC's Risk in review 2016: Going the distance
pwc.com/riskinreview

Leading businesses are automating security and privacy processes, using advanced analytics to predict and detect incidents more quickly, automating access management processes and risk and compliance management processes. They are also increasingly adopting cloud-based security solutions. Our research illustrates this, too: High Performers are more likely than other respondents to have well-defined and automated security processes, scoring more than 10 percentage points above Faster Movers and 14 percentage points above Steady Performers (companies that are highly risk-resilient but not as risk-agile).

Even more worrisome is that Faster Movers lack the critical risk-resiliency capabilities that will secure their companies in the event of a breach. High Performers are far better equipped to mobilize internal resources quickly and effectively to respond to a threat. They can immediately launch business continuity plans to keep the business up and running, and add third-party resources quickly to help as needed.

That ability to call upon third parties—your relationships with regulators, suppliers, customers and other peers in your business ecosystem—is especially critical in driving cybersecurity and privacy resiliency and agility. You need to be able to pull information from many disparate sources to build a complete picture of the cyber threat landscape. To help in this effort, the US government is encouraging companies to set up Information Sharing and Analysis Organizations (ISAOs), collaborative groups that voluntarily share threat information with one another. The European Union has approved a Network and Information Security Directive with similar goals. According to PwC's 2016 Global State of Information Security report, 56% of respondents are already sharing information with their peers.

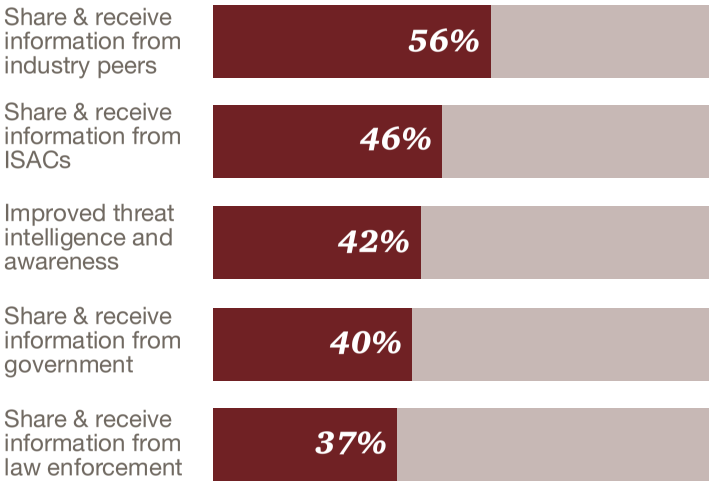
Leading companies are building threat management platforms, or threat fusion centers, where they can integrate their company's risk management intelligence with security analytics and external data from Information Sharing and Analysis Organizations (ISAOs), resulting in real-time information around current security threats. When you can crunch huge volumes of data in an integrated way, you're not only able to detect current threats quickly (the near-term speed bumps); you can actually start to predict what might happen further down the road. The better integrated your threat intelligence is about what's going on externally—what other companies in your sector are experiencing, and bigger macro trends that may affect specific countries or geographies—the greater your ability to predict what might happen to you. And that's what makes you truly risk agile, because you can get ahead of those trends and use them to your advantage.

But for most companies, just getting internal alignment is a challenge. Faster Movers are far less likely than High Performers to say their risk management program is well or highly aligned with the digital or cybersecurity team.

Figure 4

Companies are increasingly benefitting from sharing security data

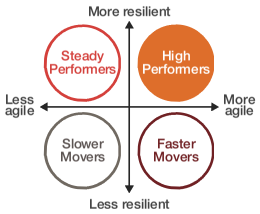
Benefits of external collaboration



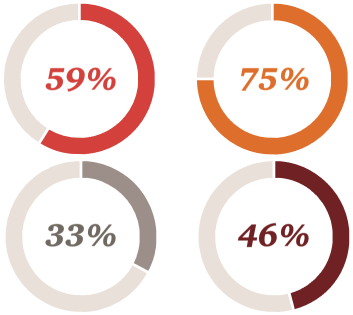
Source: PwC's Global State of Information Security 2016 report

Figure 5

High Performers are better aligned with cyber-security



Respondents who say their cybersecurity function is aligned with their risk management function today:



Source: PwC's Risk in review 2016: Going the distance
pwc.com/riskinreview

This further tells us that for many companies, the security focus is out of balance. Chief Risk Officers (CROs) have an opportunity to take a much more active leadership role in connecting the business around managing cybersecurity risk, for example:

- Engaging and coordinating the growing group of cybersecurity and privacy stakeholders, from the traditional Chief Information Officer (CIO), Chief Information Security Officers (CISO) & Internal Audit stakeholders, to Chief Marketing Officers, Chief Data Officers, Chief Digital Officers, Legal and Compliance
- Developing awareness and new skills in digital technologies, and understanding how a digital world will change their business' risk profile—including IoT, mobile, cloud, privacy regulations, ethical issues and the fast moving cyber threat landscape
- If they have not already, taking a lead in integrating cybersecurity, privacy and digital risk into the heart of their risk management programs—accepting that it will become an increasingly core part of enterprise risk management

The fact is that when it comes to security and privacy, every company has an opportunity to improve. There is a clear call to action for CROs, CSOs, Chief Technology Officers and Chief Privacy Officers to think more broadly about security and privacy, aligning their efforts across the business and helping companies understand the wider implications about their company's security strategy, rather than the specific technical response. The CRO in particular needs to take a clearer leadership role in coordinating and managing cybersecurity risk.

For additional information, please contact:

Grant Waterfall
PwC Partner, Global Cybersecurity and Privacy Assurance Leader
grant.waterfall@pwc.com
646 471 7779

www.pwc.com/riskinreview

125073_2016 jm/jc