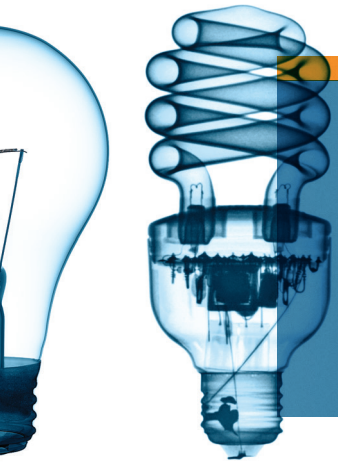
protiviti®
Face the Future with Confidence



PreView

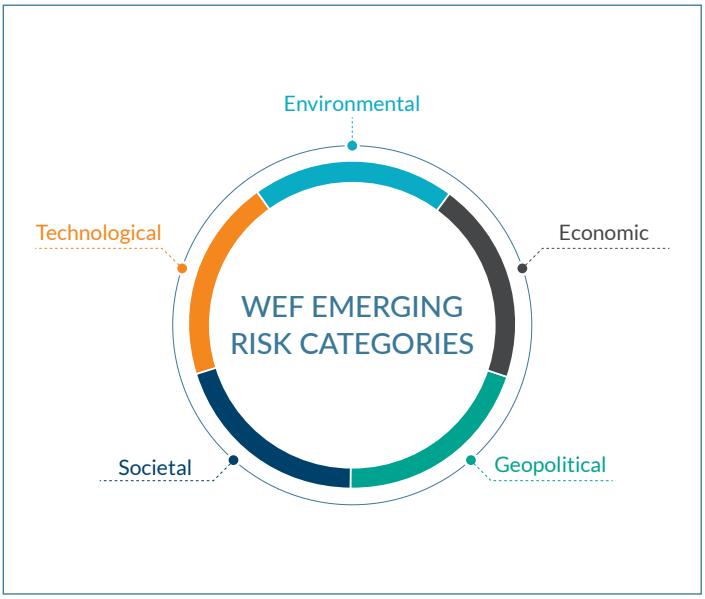
Protiviti's View on Emerging Risks

As organisations continue to evolve their risk governance practices and pursue new market opportunities, focused and relevant information about emerging risks is at a premium. The objective of Protiviti's *PreView* newsletter is to provide input for these efforts as companies focus on risks that are developing in the market. We discuss emergent issues and look back at topics we've covered previously to help organisations understand how these risks are evolving and anticipate their potential ramifications.

As you review the topics in this issue, we encourage you to think about your organisation and ask probing questions: *How will these risks affect us? What should we do now to prepare? Is there an opportunity we should pursue?*

Our framework for evaluation of risks is rooted in the global risk categories designed by the World Economic Forum (WEF). Throughout this series, we use these categories to classify macro-level topics and the challenges they present.

Inside This Issue



Cloudy With a Chance of Data Loss

Emerging Risk Category: *Technological*
Key Industries Impacted: *All*

As cloud computing globally has matured, many companies have adopted a strategy of utilising public cloud providers to run mission-critical applications. Despite periodic reports of breaches in the news, the world's largest cloud companies are focused on providing a secure cloud, and it could be argued that, in many instances, the cloud is more secure than a traditional on-premise or co-located data centre. However, organisations must be focused on managing cloud-related risks with the same attention and scrutiny with which they managed their traditional data centre risks.

The reasons for cloud breaches vary — from misconfigured files to unsecured servers to weak password protections, but the effects are generally the same: Loss of data (of customers, as well as intellectual property and confidential company data), reputation erosion, legal and regulatory challenges, and financial loss.

Cloud-related risks exist, in large part, because of cloud technology's significant benefits — including its low cost, speed of implementation, positive effects on business agility and collaborations, and more — and its widespread adoption. Twenty-one percent of files in the cloud now contain sensitive data, and the volume of sensitive data shared in the cloud has increased 53% annually, according to McAfee's 2019 Cloud Adoption and Risk Report. Successful investments in cloud-based applications have driven more enterprises to embrace third-party technology infrastructure management models, the use of cloud-based innovation platforms, and even the development of entirely cloud-based businesses.

"Customers are increasingly adopting a hybrid cloud strategy, using various delivery models for their applications, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)," according to CDW. Nearly half of current PaaS offerings are cloud-only, according to Gartner, which forecasts that enterprise spending on cloud-based offerings will surpass spending on non-cloud technology by 2022. The marketplace also is evolving, as is evident within industry-specific cloud markets where larger vendors are snapping up smaller cloud providers. This market shift has a number of implications, from posing concentration and data lock-in risks to increasing risk of data loss by making the cloud providers bigger, more lucrative targets for hackers.

To address these risks, company leaders must adopt a risk-savvy cloud approach that addresses strategy, implementation, service assurance and security. Failure to adopt such an approach raises the likelihood of experiencing higher cloud-related costs as well as data access and security issues that can expose organisations to data, reputational and financial losses. Below, we explore some of the key risks and considerations that have emerged as dominant in the cloud environment currently and which will continue to shape the risk profile of the cloud market in the future.

Key Implications and Considerations

Cloud Vendor Concentration

While cloud-based technology offerings have proliferated in most industries, others, notably the financial services industry (FSI), have witnessed significant vendor consolidation. This is a growing concern for both leadership teams and global regulators. In July 2018, the European Banking Authority (EBA) Recommendations concerning the use of cloud service providers by financial institutions took effect. "The existence of still very few credible [cloud service providers] leads to a considerable concentration risk," according to the EBA. The authority's guidance addresses five key risk areas: the security of data and systems, the location of data and data processing, access and audit rights, chain outsourcing, and contingency plans and exit strategies.

The European Savings and Retail Banking Group (ESBG) also has documented concerns related to the risks (security, concentration, reputational, regulatory and business) to which financial institutions can be exposed because of "the lack of harmonisation in regulatory approaches across different jurisdictions." The ESBG indicates that "the lack of clarity in supervisory expectations hinders the compliance with rules regarding the use, management and storage of customer information, and increases uncertainty in relation to the criteria for the approval of cloud projects." The ESBG also indicates that even the largest financial institutions often find themselves at a disadvantage when negotiating terms and conditions concerning the use and protection of company data with the handful of top (U.S.-based) cloud technology providers.

Companies of all industries can be exposed to increased concentration risks as a result of ending relationships with cloud vendors for sound reasons. Vendor risk management research, conducted annually by The Shared Assessments Program and Protiviti, shows that most companies exit third-party vendor relationships that pose high risks. Regardless of whether this de-risking is driven by high costs or other issues with the vendor, such as inability to sufficiently assess and improve vendor controls, these decisions typically result in the sharing of more organisational data with fewer external partners. Any service level agreement (SLA) changes, outages or other issues that occur among that smaller set of large cloud providers tend to have significantly larger impacts on the companies using those providers. To address concentration risks, organisations should ensure that vendors are selected and monitored in accordance with the company's cloud strategy and vendor risk management policies, sufficient vendor diversification is maintained, and SLAs are well-designed and actively managed.

Unsanctioned Cloud Services

Employee use of cloud services that are not sanctioned by the information technology (IT) function has grown steadily in the five years since CSO Online posted an article warning IT leaders to "Forget BYOD — it's now BYOC." Three years ago, an NTT Communications Corporation survey of 500 IT decision-makers determined that 77% of companies commissioned a cloud service without the IT department's involvement. The practice is so common and pervasive, that the news of White House adviser Jared Kushner using unsanctioned, insecure cloud-based messaging service WhatsApp to communicate with foreign contacts elicited either a shrug or an outrage determined only by the political leanings of the reader. By year 2020, Gartner expects "shadow" IT resources to be the root cause of one-third of successful cyberattacks on enterprises. In addition to the security risks, shadow IT poses

a potential unrelated legal risk, for example, when a legal hold is placed on company or customer data or it is requested for investigative support (see "Legal Holds" below). When employees use shadow cloud services that are not subjected to IT oversight and governance, considerations regarding legal holds are almost always neglected. To limit "bring your own cloud" (BYOC) risks, organisations should continually educate the workforce on IT governance policies (and the risks of all forms of shadow IT) and perform regularly scheduled penetration testing to understand the use of unauthorised cloud services and how these risks can be remediated.

Data Location — and Data Ownership

To make their offerings competitively priced, some cloud vendors have deployed creative ways to keep costs — or the appearance of costs — low. In some arrangements, vendors treat customer data stored on their servers as an asset to be aggregated and sold to retailers, search engines and other third parties. Language concerning data ownership and data location may be buried in the contract or addressed in vague terms. These vendor tactics bring into focus the need for clear, well-defined and well-understood SLAs.

Imprecise data ownership stipulations should be identified and challenged by cloud customers prior to entering into a vendor relationship. Often, however, the teams procuring cloud offerings are not sufficiently educated on data ownership risks, which can result in cloud providers negotiating outright ownership of the customer data on their servers. If customer data includes regulated information under, for example, the General Data Protection Regulation (GDPR), and the cloud provider fails the GDPR-specified data privacy provisions by reselling the data down the line, the customer with whom the data originates faces the GDPR compliance violations.

To limit risks associated with data ownership and location, organisational cloud strategies and governance should emphasise ongoing education concerning these issues. These strategies also should contain specific policies regarding data ownership and location.

Legal Holds and Investigative Support

How data is stored and controlled by cloud providers also affects the ease and speed with which cloud customers can respond to pending litigation that generates legal holds involving that data. A legal hold requires an organisation to preserve records and information related to the legal matter. While cloud vendors should have tools and processes in place to respond swiftly to legal holds issued to their customers, this capability is frequently overlooked during the due diligence and provider selection process and the finalisation of SLAs and contracts.

Some vendors offer additional investigative support for legal holds; this support typically involves the vendor helping the client secure and process relevant data. The legal hold risks should also be considered when negotiating data ownership (as discussed above). Legal holds issued to a cloud provider could involve customer data, locking it up or making it available in violation of the customer's policy. To address risks associated with legal holds, vendor selection processes should include mechanisms for determining prospective cloud vendors' ability to respond quickly to legal hold notices, preserve data and information in accordance with these types of requirements, and provide additional investigative support.

Vendor Lock-In

A startling cloud-related note was nestled in Snapchat parent company Snap's IPO filing announcement a couple of years ago. Snap reported that it was bound by contract to "spend $2 billion with Google Cloud over the next five years and have built [its] software and computer systems to use computing, storage capabilities, bandwidth, and other services

provided by Google." Snap also reported that Snapchat uses some Google services "which do not have an alternative in the market." As Mesosphere CMO Peter Guagenti noted in a post at the time, "Google now has them in handcuffs, and there's little Snap can do to change that without having to invest a tremendous amount of money to free themselves." Snap is hardly alone. Many companies find themselves bolted to a cloud provider due to complex technical arrangements (e.g., storing data in proprietary formats), specific contractual terms and other dependencies. "Cloud providers also often make the movement of data from the cloud to an on-premise centre or another cloud vendor difficult, complex, and expensive," according to *Forbes* contributor Dan Woods. "The reason for this is clear — it's in their interest for you to keep your data with them, as they want their customers to 'stick' to them in perpetuity." When vendor lock-in exists, companies can be exposed to significant maintenance and service price increases while their performance, to varying degrees, is wedded to the performance of their cloud vendor. As with other cloud risks, vendor lock-in should be addressed through effective vendor selection processes, SLAs and ongoing performance monitoring.

Areas of Focus to Mitigate Cloud Risk

The risks highlighted above should not suggest that cloud is an unsafe choice for companies. For many companies, the move to a well-managed cloud platform actually decreases risk. Appropriate vendor selection criteria, well-crafted SLAs and effective IT and vendor risk management governance and controls go a long way toward mitigating the risks discussed above. These processes should be part of a comprehensive, methodical approach to cloud adoption and ongoing cloud risk management that also includes architecture considerations, ongoing monitoring, change management protocols and other mechanisms. Although these approaches vary, an effective framework addresses the following four areas:

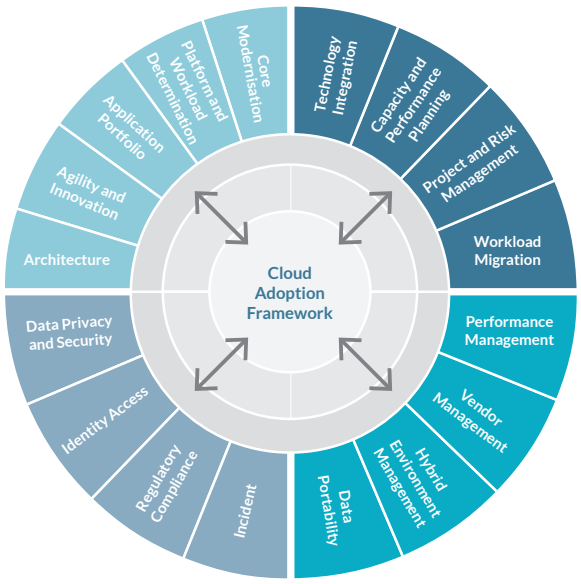
• • • Considerations for Cloud Computing

STRATEGY

Cloud computing strategy is about deploying the right application services on the right architecture, based on the risk appetite of the organisation. This process is usually not as simple as migrating from an existing technology platform to the cloud. It requires a different way of designing, deploying and managing IT services.

SECURITY

Security remains a major concern with cloud implementation, with four key areas of focus: data privacy, access management, regulatory compliance and incident management.



IMPLEMENTATION

The implementation of the cloud and the day-to-day management of cloud operations should be owned by the organisation's service operations function to ensure issue resolution and minimal disruption of the technology stack.

SERVICE ASSURANCE

To safeguard cloud services, firms need a strong service assurance function, which includes vendor management. Core legacy systems may need to be modernised or refreshed to ensure proper interaction with the cloud.

Source: "Cloud Adoption: Putting the Cloud at the Heart of Business and IT Strategy," Protiviti, 2017. https://www.protiviti.com/US-en/insights/cloud-adoption-putting-cloud-heart-business-and-it-strategy

Spotlight: Tape Wars, and Why Cloud Storage Costs May Soar

Just as cloud customers strive to mitigate vendor concentration risks, so do cloud providers. Concentration risks for cloud vendors stem from their suppliers of cloud storage backup. The number of manufacturers that produce the magnetic tape used to securely store back-up data has shrunk from six to two, Sony and Fujifilm, during the past several years. What's more, the two manufacturers are trying aggressively to reduce their market down to a single provider. Each company has spent heavily in attempts to ban the other from importing tapes to the U.S., according to Bloomberg Businessweek.

The two corporations also have squared off against each other over claims of patent infringement. This heated battle may be bad news for cloud vendors and their enterprise customers. Although the magnetic tape was invented a century ago, it remains the standard for back-up data storage because it can endure for three decades and, thanks to comparatively recent improvements, can store vast amounts of data. If the number of global manufacturers of magnetic tape declines to one, that company could levy massive price increases. This would translate to much higher costs for cloud providers that they would likely pass on to their customers.

For more on escalating cloud costs, see "On the Radar" on page 17.

"Cloud computing is now an intrinsic part of the enterprise landscape. As cloud adoption is driven increasingly by business transformation needs and as businesses respond to demands levied by rapidly evolving consumer behaviours, changing business models and the need to respond to opportunities and risks arising from new market entrants, the processes and practices for managing cloud-related risks must mature."

— Eric Winton, Managing Director, Protiviti

Cybersecurity: The Escalating War

Emerging Risk Categories: *Technological, Economic, Geopolitical*
Key Industries Impacted: *All*

By 2021, cybercrime is projected to cost the world $6 trillion annually, according to "The Cybersecurity Imperative," a recent research study. The U.S. State of Cybercrime survey indicates that nearly one in four organisations suffered greater financial losses from cyberattacks in 2017 than in the previous year. More than 4,000 ransomware attacks strike companies daily, according to FBI research. Advanced persistent threats (APTs), in which cyber criminals gain unauthorised access to company networks and remain undetected for weeks or months, are increasingly problematic: On average, it took companies 191 days to identify a data breach in 2017. That's a long period of time, during which much damage can occur.

If the numbers do not evoke a sense of urgency, they should: Gartner forecasts that 60% of digital businesses will suffer a major service interruption from a cybersecurity breach by 2020. Recent conversations between regulators and the financial services industry focusing on operational resilience are driven in large part by major cyber disruption concerns, as well.

Organisations' adoption of advanced technologies, increased data-sharing with third-party vendors, and the growing sophistication of external cyberattacks are the primary factors responsible for escalating cyber risk. Add an abundance of political motivation and state-level funding of such attacks, and it becomes readily apparent that cyber risk is now one of the top threats to nations and organisations alike.

Digital Maturity and Cyber Risk

Each additional Internet-connected sensor embedded in a device, piece of manufacturing equipment or product poses a new cybersecurity risk. The potential exposure is staggering, considering that Gartner expects more than 20 billion connected devices to be in use by next year. Artificial intelligence (AI), blockchain and other advanced technologies that drive digital maturity create additional cybersecurity risks. As companies become more digitally mature, their odds of experiencing a $1 million-plus cyberattack loss event increases, according to The Cybersecurity Imperative research. However, digitally mature companies with the most advanced cybersecurity capabilities are far less likely to experience an event of that magnitude compared to digitally mature companies with the least advanced cybersecurity programs. In other words, if a company evolves its digital maturity but neglects to evolve its cybersecurity capabilities at the same pace, the results could be catastrophic.

Third Parties

Sixty-one percent of U.S.-based companies experienced a data breach caused by one of their vendors or third parties last year, according to a Ponemon Institute survey of chief information security officers (CISOs). These types of attacks struck Best Buy, Delta, Saks Fifth Avenue and numerous others by infiltrating point-of-sale, customer service and other types of third-party technologies and services. While only 20% of business leaders

are currently concerned about cyberattacks via third parties, 70% believe they will have to address this risk within the next 18–24 months, an increase of 247%. The finding in a recent Vendor Risk Management (VRM) survey, that companies' VRM programs today are barely keeping up with the expanding threat landscape, adds to the challenge.

State-Sponsored and Sophisticated Attackers

"States are using the tools of cyberwarfare to undermine the very foundation of the Internet: trust," warns a recent *Foreign Affairs* article. "They are hacking into banks, meddling in elections, stealing intellectual property, and bringing private companies to a standstill. The result is that an arena that the world relies on for economic and informational exchange has turned into an active battlefield."

• • • Key Implications and Considerations: Tactics, Targets and Defence

More Sophisticated Attacks

Perpetrators of cyberattacks include states, terrorists, criminals, insiders and activists. While insiders remain a surprisingly persistent risk, the cyberattack capabilities of nation states and organised criminal groups are rapidly maturing. An increasingly sophisticated cyberattack supply chain includes innovative criminals in countries such as Russia and Romania selling ransomware and more advanced cyberattack tools to extortionists in regions such as West Africa, who then target companies quite effectively: roughly 40% of ransomware victims pay the ransom. No longer content with pilfering credit card and personally identifiable data, attackers continually look for new ways to rob and destabilise organisations and nations. As companies strengthen their ransomware, phishing and distributed denial of service (DDoS) countermeasures, attackers add new modes to their arsenals, including IoT botnets, cryptojacking, AI-powered malware, spear phishing and man-in-the-middle attacks.

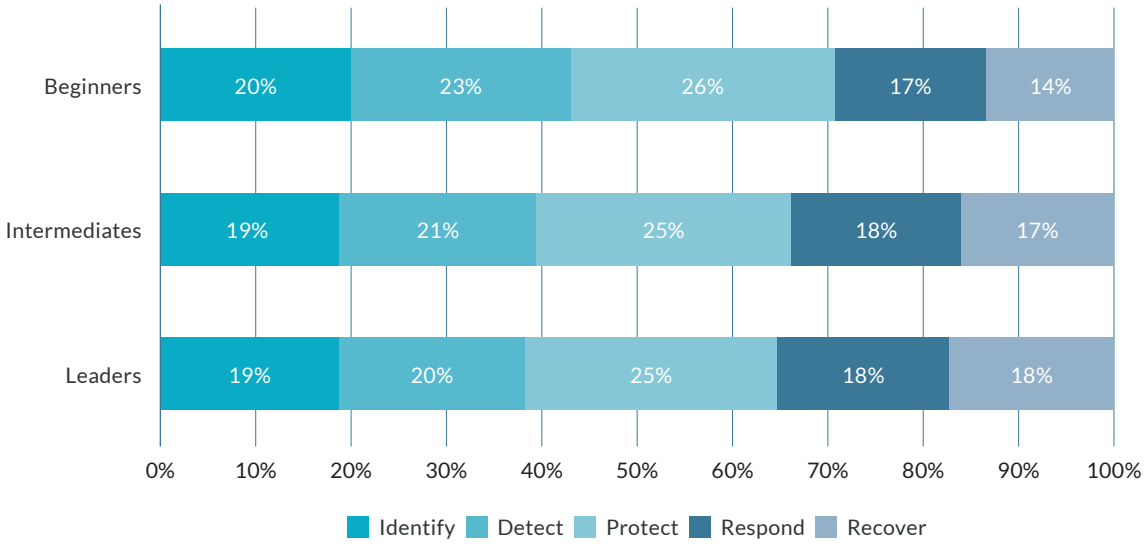
All Industries Are Vulnerable but Costs for Some Are Much Higher

State-sponsored cyberattackers traditionally targeted critical infrastructure industries (and related government agencies) such as utilities, communications, healthcare and financial services. Recently, however, these attacks have extended to new targets, including the Democratic National Committee in the U.S., as a means of undermining trust in longstanding institutions. Some states, like North Korea, have launched attacks against organisations (e.g., Sony Pictures) as a means of payback against perceived slights or to generate tens of millions of dollars via theft. While it is difficult to quantify accurately the theft of U.S. intellectual property from cyberattacks, the Center for Strategic and International Studies estimates that the U.S. loses $20 billion to $30 billion annually as a result of Chinese cyber espionage that targets businesses via IP theft and financial crimes.

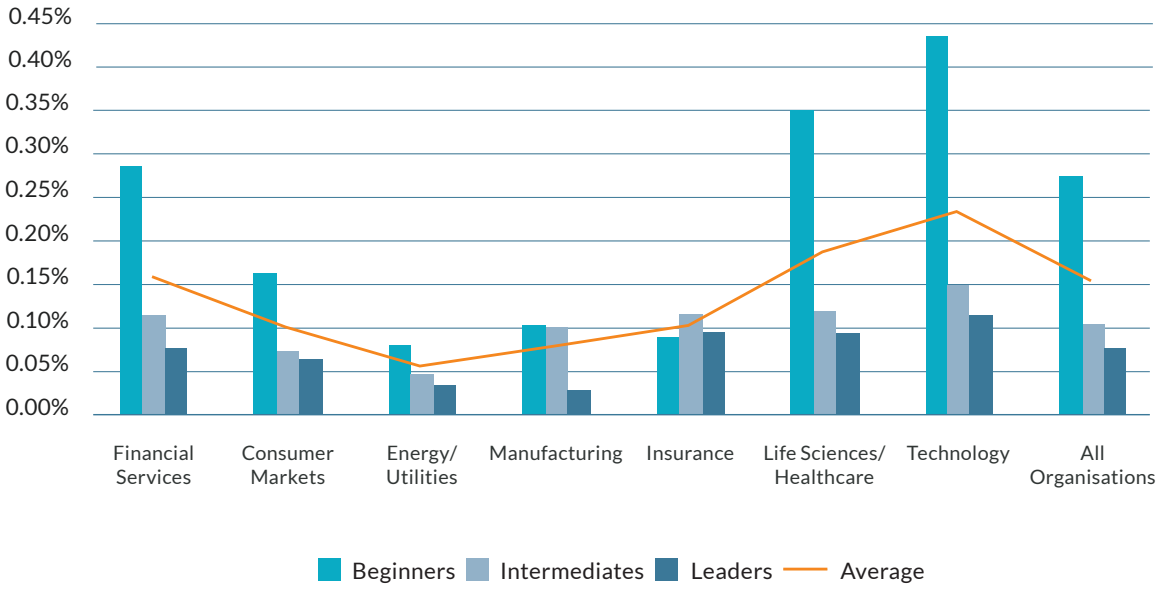
Critical infrastructure companies continue to warrant especially stout cybersecurity capabilities to limit the potential human toll of attacks, but all industries and companies are targets. That said, companies within the technology, life sciences/healthcare and financial services industries (companies in possession of valuable IP, personal or financial information) spend more on cybersecurity (as a percentage of revenue) than companies in the consumer, energy/utilities, manufacturing and insurance industries, according to The

Cybersecurity Imperative research. Among all companies, those with advanced cybersecurity capabilities tend to spend significantly less on their programs, as a percentage of their revenue, than companies with the least sophisticated cybersecurity programs. The research also suggests that companies in the early stages of their cybersecurity improvement journeys tend to invest mostly in protection, detection and identification against/of breaches. Cybersecurity leaders, on the other hand, tend to invest more in response and recovery activities. The conversation among cybersecurity experts is also shifting toward response and recovery, implying that they view resilience to cyberattacks in terms of surviving them with minimal damage as opposed to preventing them altogether.

Cybersecurity Spending by Maturity and NIST Category



Cybersecurity Spending as a Percentage of Revenue



Source: "The Cybersecurity Imperative," Protiviti and ESI Thought Lab, 2018. https://www.protiviti.com/US-en/insights/cybersecurity-imperative

Countermeasure Strategies

An effective cybersecurity capability requires recognition of a fundamental risk principle: "as more and more organisations embrace digitisation," according to CIO, "they inevitably become prey to new cyber-dangers and, in turn, need to put much greater emphasis on the availability, stability and resilience of their IT systems." Optimising the business benefits of new technology while minimising its cyber risk requires a cybersecurity program that addresses the following success enablers:

- **The use of a framework.** Most cybersecurity programs rely on a framework that designates how organisational data will be identified and protected; how the organisation will respond to attacks; and how the company will recover when a cyberattack disrupts business. While these structures vary, many organisations model their cybersecurity programs on a handful of widely used framework standards, such as NIST or ISO/IEC 27000. The business-focused NIST framework, which guides organisations in their management of cyber risk and communication of the risks to senior management and the board, organises cybersecurity activities into five functions. Of these functions, most companies currently perform most effectively on protect and detect activities while performing the least effectively on identify, respond and recover activities — but they need to build these capabilities as well to respond to the shift in regulatory focus toward post-cyber event resilience.

Percent of Companies Reporting Progress Against NIST Categories

Identify | Protect | Detect | Respond | Recover

Top Seven NIST Categories		NIST Function	Bottom Seven NIST Categories		NIST Function
Limit access to physical and logical assets to authorised users and devices.	39%	Protect	Prioritise the organisation's objectives, stakeholders and activities.	18%	Identify
Analyse incidents to ensure effective response and support recovery.	39%	Respond	Train staff and partners in cybersecurity awareness and to perform duties in line with policies and procedures.	17%	Protect
Monitor information systems and assets to identify cybersecurity events.	36%	Detect	Identify data, data flows, devices, personnel and systems that could affect cybersecurity.	16%	Identify
Maintain security policies and procedures for protecting information systems.	35%	Protect	Perform maintenance and repairs of industrial control and information systems according to policies.	14%	Protect
Manage data in line with risk strategy to protect integrity and availability of information.	34%	Protect	Detect anomalous activity and understand the potential impact of events.	13%	Detect
Establish priorities, risk tolerances and assumptions.	34%	Identify	Understand policies and processes to manage and monitor organisation's regulatory, legal, risk and operational requirements.	11%	Identify
Identify cybersecurity risk to organisational operations and organisational assets.	32%	Identify	Act to prevent expansion of an event, mitigate its effects and resolve the incident.	11%	Respond

Source: "The Cybersecurity Imperative," Protiviti and ESI Thought Lab, 2018. https://www.protiviti.com/US-en/insights/cybersecurity-imperative

- **Risk quantification and integration.** A risk-based approach to cybersecurity is crucial, given that each company will be affected by the same attack differently based on its assets and risk appetite. Within cybersecurity programs, quantitative risk analysis helps translate threats (and their impacts) into financial terms that can facilitate the prioritisation of cyber risks, both individually and in comparison with other business risks. This analysis also helps drive cybersecurity's integration with enterprise risk management.
- **Information sharing among industry, governments and countries.** As the use of cyber warfare continues among states and terrorists, national collaborations and information-sharing among government entities and private industry (like this UK initiative launched in late 2016) are bound to increase. In the U.S., there are numerous industry-specific information sharing and analysis centers (ISACs) that foster collaboration on cybersecurity issues and practices for companies in similar industries (e.g., automotive, financial services, healthcare, oil and gas, and more).

  More cybersecurity information and practices sharing is also needed on a global scale, and multinational organisations are stepping up to address this need. The Global Cyber Alliance (GCA) is one example of an international, cross-sector effort. The GCA focuses on the most prevalent cyber risks individuals and businesses face by developing and making available practical, real-world solutions to fortify global cybersecurity.
- **War games and joint exercises.** Finally, "war games" and joint testing exercises for large-scale cyber scenarios are sponsored by industry organisations, such as the Security Industry and Financial Markets Association (SIFMA), with the participation of government entities. Such exercises are important for ensuring the resilience of an entire sector and its infrastructure, whether finance, transportation or energy.

"Two realities are facing companies in today's market. First, the protection of critical company and customer information is a business requirement and is fundamentally about preserving reputation and protecting enterprise value. Second, even the best cybersecurity programs will experience failure and expose some assets that management and directors would like to protect. That is why confidence in security and privacy is achieved by knowing all the things that can happen and preparing both proactive and reactive solutions to address them."

— Scott Laliberte, Managing Director, Protiviti

Spotlight: Is AI or Dale Carnegie Your Next CISO? The Answer Is "Both."

Imagine an AI-fueled cybersecurity tool that combs through a company's entire IT environment 24/7 to sniff out suspicious patterns and stop malicious hacks before they inflict damage. While that scenario could soon be reality, and AI is most certainly suited to play certain valuable roles in the cybersecurity arsenal of companies, it is unrealistic to expect the technology to replace humans any time soon. As companies integrate AI into their cybersecurity programs they would do better to focus on talent acquisition with the proper skill sets to manage and improve implementation of the technology. To illustrate, the following three critical aspects of the CISO's ecosphere cannot be addressed by AI effectively:

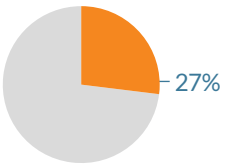
- **CIOs and CISOs play a critical communication role to the board of directors on cybersecurity matters.** According to the VRM survey cited earlier, board engagement is a crucial enabler of both a strong cybersecurity capability and a mature third-party risk management program (an increasingly important driver of cybersecurity effectiveness). These eight considerations for corporate directors — which include gauging their confidence in the cybersecurity information presented to them, focusing on the adverse business outcomes, and extending cybersecurity beyond the company's four walls, among others — can help boards understand and support cybersecurity programs more effectively. In addition, cybersecurity leaders need to persuade C-suite executives and board members of the magnitude of cyber risks and the level of investment cybersecurity programs require. A black box can't do that.
- **Increasingly, CISOs operate more like chief talent officers than technology officers.** The cybersecurity skills shortage is getting worse. A CSO survey finds that half of organisations describe access to this expertise as a problem. What's more, board members identify cybersecurity and the ability to attract and retain top talent (including IT and cybersecurity skills) as two of the overall top-five risks facing their companies. The skills needed to prevail in today's cyber environment are a broader set than simply coding and testing, and include data analytics, data visualisation, risk analysis, privacy, regulatory compliance and project management. And it is the CISO's job to deploy innovative talent sourcing, development and retention approaches to gain access to this range of talent.
- **AI and other advanced technologies can be used on offence and defence.** AI has the valuable potential to help organisations spot and end attacks or, in some cases, to prevent them from occurring. However, just as cybersecurity leaders are evaluating how to integrate AI into their cybersecurity programs, bad actors are assessing how to deploy AI tools to break down organisational defences. The virtual "battle of the bots" between cyber thugs and information security capabilities will intensify given the pace of technological advances and the widespread adoption of the Internet of Things (IoT). The human CISO, however, remains the chief strategist in that battle as only she or he can orchestrate, fund and direct the deployed technology.

The Quest for the Millennial Spend

Emerging Risk Categories: *Societal, Economic*
Key Industries Impacted: *Financial Services, Real Estate, Consumer Products and Services, Transportation*

What happens if consumption and growth stagnate for a generation? Millennials are now between 23 and 38 years old, the age at which most members of prior generations were buying homes and raising families. But millennials came of age during the Great Recession, and, according to the World Economic Forum, "prosperity has plummeted for young adults in the rich world." From the same source, millennials in western economies earn significantly less than national averages, and their disposable incomes can be much lower than those of retired adults. By next year, this financially-strained generation will account for 35% of the world's workforce.

As incomes fall, younger consumers defer or decline pursuit of marriage, children and home purchases, and are more likely to max out their credit cards than older generations. In addition, a majority of millennials believe they are more concerned about protecting the environment than older generations, a view that can have a marked impact on personal preferences and lifestyle decisions. As a result, economies worldwide are feeling the effects of these behavioural patterns. Businesses that succeed in serving this generation will be those that are alert to differences in economic conditions worldwide, and seek out the pockets of opportunity. The glut of research data on millennials depicts a diverse market that defies any global generalisation.



Millennials account for 27% of the world's 7.4 billion population.

There are 1.8 billion millennials in the world, and 86% of them live in emerging and developing countries (in more advanced economies, lower birth and death rates reduce their prevalence). Over a billion millennials live in Asia — and Chinese millennials number more than the entire population of the U.S. (where there are only slightly over 75 million millennials). It's tempting to think these numbers are static: they're not. Stronger economies will see millennial populations swell as young adults from disadvantaged parts of the world seek better economic opportunities abroad.

"Economists and other observers may argue endlessly over the true drivers of economic growth, e.g., consumption, savings, investment, international trade, public policy choices or all of the above. Regardless of where that debate leads, the behaviour of millennials and its impact on the generation's spending, savings or investing habits are factors that cannot be ignored as companies source capital and evaluate, segment and target their markets."

— Sharon Lindstrom, Managing Director, Protiviti

A World Tour of Millennial Markets

Asian millennials, considered altogether, number over 1 billion — but they cannot be considered collectively; Asia's markets are large and diverse. In addition to massive millennial populations in India and China, smaller countries have growing millennial markets as well. However, the buying power of millennials in India and China is what sets these two markets apart.

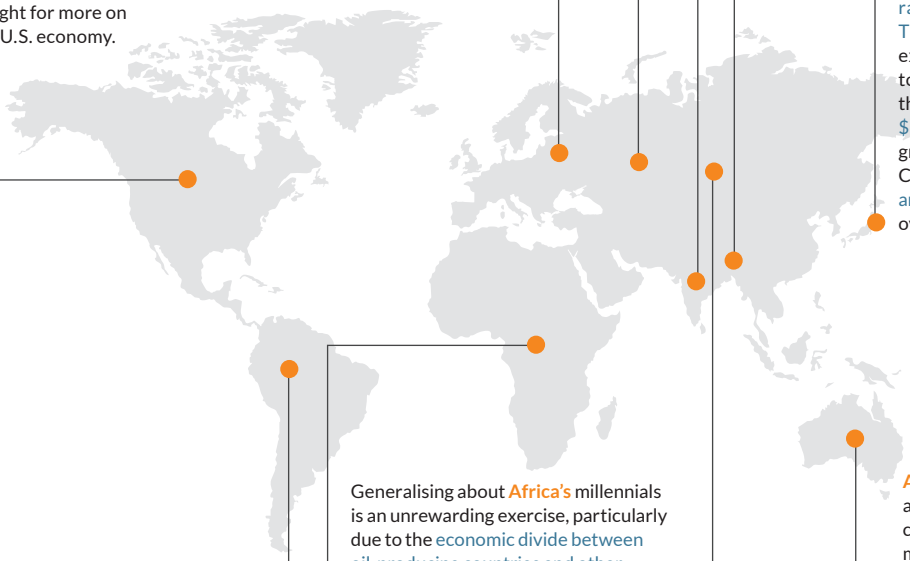
India is home to 440 million millennials, who make up a third of the overall population, and 46% of the workforce there. India's economy has grown steadily for the last 50 years, and has averaged over 7% growth in the last decade. Its GDP was nearly $2.6 trillion in 2017, and consumer spending was 57%. Millennial income averaged more than 10% higher than for people over 45 in 2015, and the increase in India's working age population will constitute over half of the total increase in the working population in Asia over the coming decade.

In Europe, about 102 million millennials constitute only 20% of the population. European economies are difficult to generalise, but youth unemployment tends to be higher than for older generations. According to a 2016 Eurobarometer survey, 57% of European youth believe "the young have been marginalised and excluded from economic and social life."

Millennials in the United States constitute nearly a quarter of the total U.S. population, at over 75 million. In 2016, millennials became the majority of the U.S. workforce, graduating into a market of high unemployment, lower salaries and higher costs of living. In the U.S., over 30% of millennials have no savings at all. See our Spotlight for more on millennials in the U.S. economy.

Other markets where opportunities to introduce new, high-value products will be those where millennials are forecast to enjoy high average incomes, paired with increasing aggregate incomes. The most promising of these markets include Bangladesh, Indonesia, the Philippines, and Thailand.

In Japan, pessimism about their economic futures is reportedly rampant among millennials. Thirty-seven percent of them expect never to retire, compared to 12% of U.S. millennials. While the GDP in Japan was just over $6 trillion in 2017, its annualised growth rate was only 1.7%. Consumer spending has remained around 55%, with small variances, over the past few years.



Australia stands out as an anomaly in the developed countries' economic outlook for millennials. Australians aged 25 to 34 have actually enjoyed increases in their incomes compared to the population average. They have also done better than people the same age in other countries.

Latin America and the Caribbean are home to 77 million low-income millennials, largely neglected by market studies which tend to focus on affluent populations. While affluent markets certainly yield rewards, so too can very large, base-of-pyramid markets. By next year, 35 million low-income people in Latin America will make their way into the middle class, and many of those will be millennials.

Generalising about Africa's millennials is an unrewarding exercise, particularly due to the economic divide between oil-producing countries and other economies. Countries not dependent on oil are reporting positive GDP growth, generally above 6%. Africa has a population of nearly 1.3 billion, an astonishing increase from only 140 million in 1990. Millennials constitute 37% of the population: Africa is the youngest of all the continents. By 2050, the continent will be home to 38 of the 40 youngest countries. Africa is also the only region where the share of the working-aged population is projected to continue to rise over the next 15 years, according to the World Bank. However, while 10-12 million new workers enter African workforces each year, only 3 million formal jobs are created annually at the present time. Although at present this is causing migration pressures as labor supply far outpaces demand on the continent, there are considerable opportunities for future economic growth through investment in education and job training, as well as infrastructure.

China is home to 415 million millennials. Consumption in China is now 40% of a GDP that exceeds $12 trillion, thanks to recent economic policy reforms that shifted emphasis from investment to consumption. In the first three quarters of 2018, consumption accounted for 78% of the country's GDP. By 2035, the aggregate income of millennials there will surpass the aggregate millennial income in the U.S. According to a study released by Chinese technology giant Tencent Holdings last September (before U.S. trade policy shifted), Chinese customers were projected to account for 40% of global luxury goods sales by 2024, with those aged 18-30 accounting for 58% of luxury goods buyers.

Key Implications and Considerations

People grow up, enter the job market, get married, buy houses and start raising children. Consumer-driven economies have historically relied on this age-old pattern to fuel sales of housing and consumer products. But millennials worldwide — generally speaking, and for a variety of reasons — cannot or do not take those steps according to prior generations' timelines. Nevertheless, millennials are becoming the core customer base for many industries, from home construction, cars and other durable goods, to housewares, clothing and telecommunications services. How industries react and what new products they develop will determine how successful they will be in marketing to this generation.

Housing and Real Estate

The housing industry provides work for millions of people globally. When construction slows, unemployment rates rise. Declining home sales depress prices, reducing the availability of home equity loans. With less available credit, consumer spending falls.

In the U.S., homeownership remains a marker of financial security and a foundation for wealth-building, but a wide range of factors keep millennials out of the housing market:

- **Student loan debt:** About two thirds graduated with debt, and the average debt among graduates is over $28,000 — and that excludes the borrowers who did not graduate.
- **High rents:** The preference (or need to be close to well-paying jobs) to live in cities incurs higher costs, and rents in urban markets can preclude saving toward a home purchase.
- **Higher home prices and increasing mortgage rates:** According to CNBC, one in three millennial homeowners in the U.S. withdrew money from or took loans against their retirement accounts to finance the down payment on a home. Further, slightly more than 40% of millennial homeowners said they had regrets after they purchased a home because they felt stretched financially.
- **Fear:** Having grown up witnessing foreclosures and evictions in real life and on the news makes the prospect of investing in real estate a scary proposition for many millennials.

Despite the above statistics, 72% of U.S. millennials say owning a home is a "top priority." Thus, it isn't a lack of desire or financial literacy that keeps millennials out of the housing market — it's simply out of reach for many of them. See the Spotlight on the next page for how some construction and real estate companies are helping millennials get closer to homeownership.

Consumer Products and Services

The millennial's ideal home appears to have a smaller footprint in a lively urban setting, with a flexible, open floorplan. Consumer products manufacturers, especially those of home appliances, furniture and clothing, should study the preferences of their consumer base and deliver products for a smaller-footprint, lower-income lifestyle. While the volume of products sold may be reduced, there is an opportunity to innovate and build loyalty with smart, versatile and green or recycled products that fit the millennial budget and sensibilities.

Transportation

Car sharing companies and services, such as Zipcar, Gig Car Share and Get Around, have proliferated to cater to millennials who do not own homes with garages or cannot afford the full expense of a vehicle. Fifty-three percent of millennials say they cannot afford a car. This presents opportunities for new financial products such as short-term car leases and privately funded shuttles to supplement public transportation. Governments can also achieve their goals of increasing the amount of urban housing and reducing pollution by partnering with private investment, especially real estate companies, for public transit projects, including bike infrastructure.

Spotlight — Helping Millennials Buy a Home

Metrostudy's recent report on housing trends says builders can counter the factors that keep millennials out of the real estate market and boost home sales by constructing smaller, factory-built homes, offering terms that keep payments low for the first years of ownership, and reducing association fees in new complexes to attract millennial buyers. Bolstered by the abundance of data available for this highly-scrutinised population, builders are beginning to deliver.

Builderonline lists several strategies for getting millennials into a house of their own – offer basic value, skip the luxuries, assist with loans that take into account millennials' student debt payments, and offer "moving up" incentives such as trading for a bigger home, as opposed to selling and buying. Additionally, real estate companies can provide support in the form of educational materials, expertise and guidance through the home-buying process.

Even though millennials are more likely to live in cities than other generations, more millennials are moving to the suburbs because of lower costs. Companies like Zillow are marketing a different kind of suburb to those potential buyers — one that incorporates shopping, services and entertainment, as opposed to the traditional, car-oriented, shopping-deprived suburb of prior generations.

There are some sweet spots noted here. Firms that seek to grow by engaging the millennial generation that is now shaping the global economy and culture must look beyond today's established markets. Businesses that are agile enough and bold enough to seek out the most promising young markets, understand their needs and build loyalty with them through innovative products, services and financial models that satisfy those needs will be the winners in the millennial economy.

On the Radar

Focus on Operational Resilience

In today's dynamic business environment, rapid innovation, progression in business digitalisation and an increased reliance on third-party vendors and downstream providers for critical business services pose daily operational risks to companies. In this environment, enhancing a firm's operational resilience has never been more critical.

Operational resilience is the ability of an organisation to withstand adverse changes in its operating environment and continue the delivery of business services and economic functions. While business continuity, a related concept, has been an important element of the risk management of organisations for a long time, the concept of resilience differs in that it takes into account not just the business itself but the role the business plays in the critical economic functions of society as a whole. Increasingly, companies recognise that traditional business continuity and disaster recovery playbooks can no longer be relied upon to tackle wide-scale disruptions, including cybersecurity-related outages, and that certain events can threaten the stability of an entire sector by crippling sector-critical service providers, their customers and their business partners.

Driven by the growing angst, and a rash of outage incidents at banking institutions last year, regulators of the financial sector were the first to focus on the concept of operational resilience. In 2018, the Bank of England issued a discussion paper highlighting operational resilience as a top priority for financial institutions. But these risks are not limited to the financial services industry. Other sectors — particularly technology, utilities, oil and gas, and healthcare — are equally vulnerable. These industries, which rely heavily on third-party service providers and are at increased risk for cyber disruption, would be prudent to understand their unique operational resilience issues and consider how operational resilience standards could apply across industries.

In a future issue of *PreView*, we will explore the common challenges and recent breakthroughs related to operational resilience as well as solutions that all organisations can leverage to support their resilience efforts.

Escalating Cloud Costs

As we outlined in "Cloudy With a Chance of Data Loss," companies are embracing the considerable benefits of the cloud despite certain risks. Many of these companies make the decision to migrate to the cloud lured by the promise of lower total cost of ownership for SaaS applications and infrastructure. The allure of evergreen software, paying only for what is used, and managing usage peaks and valleys to control costs is often a key factor in defining a cloud strategy. However, if companies do not manage usage, access and architecture decisions tightly, there is the risk that cost savings are not realised, but combined with cloud migration expenses, actually lead to an increased total cost of ownership over time. This is a risk we will continue to watch and address in more detail in a future issue of *PreView*.

Continuing the Conversation

The risk areas summarised in this issue will continue to evolve, and there is no question that new risks will emerge and affect organisations globally. We are continuing the discussion we've started in this newsletter on our blog, The Protiviti View (blog.protiviti.com). Our blog features commentary, insights and points of view from Protiviti leaders and subject-matter experts on key challenges and risks companies are facing today, along with new and emerging developments in the market. We invite you to subscribe and participate in our dialogue on today's emerging risks. You can also find additional information on our microsite, protiviti.com/emerging-risks.

About Our Risk Management Solutions

Protiviti's risk management professionals partner with management to ensure that risk is appropriately considered in the strategy-setting process and is integrated with performance management. We work with companies to design, implement and maintain effective capabilities to manage and respond to their most critical risks and address cultural and other organisational issues that can compromise those capabilities. We help organisations evaluate technology solutions for reliable monitoring and reporting, and implement new processes successfully over time.

Contacts

Cory Gunderson
Executive Vice President
+1.212.708.6313
cory.gunderson@protiviti.com

Jim DeLoach
Managing Director
+1.713.314.4981
jim.deloach@protiviti.com

Andrew Clinton
Executive Vice President
+44.20.7024.7570
andrew.clinton@protiviti.co.uk

Matthew Moore
Managing Director
+1.704.972.9615
matthew.moore@protiviti.com

Jonathan Wyatt
Managing Director
+44.20.7024.7522
jonathan.wyatt@protiviti.co.uk

Jason Daily
Managing Director
+1.312.476.6420
jason.daily@protiviti.com