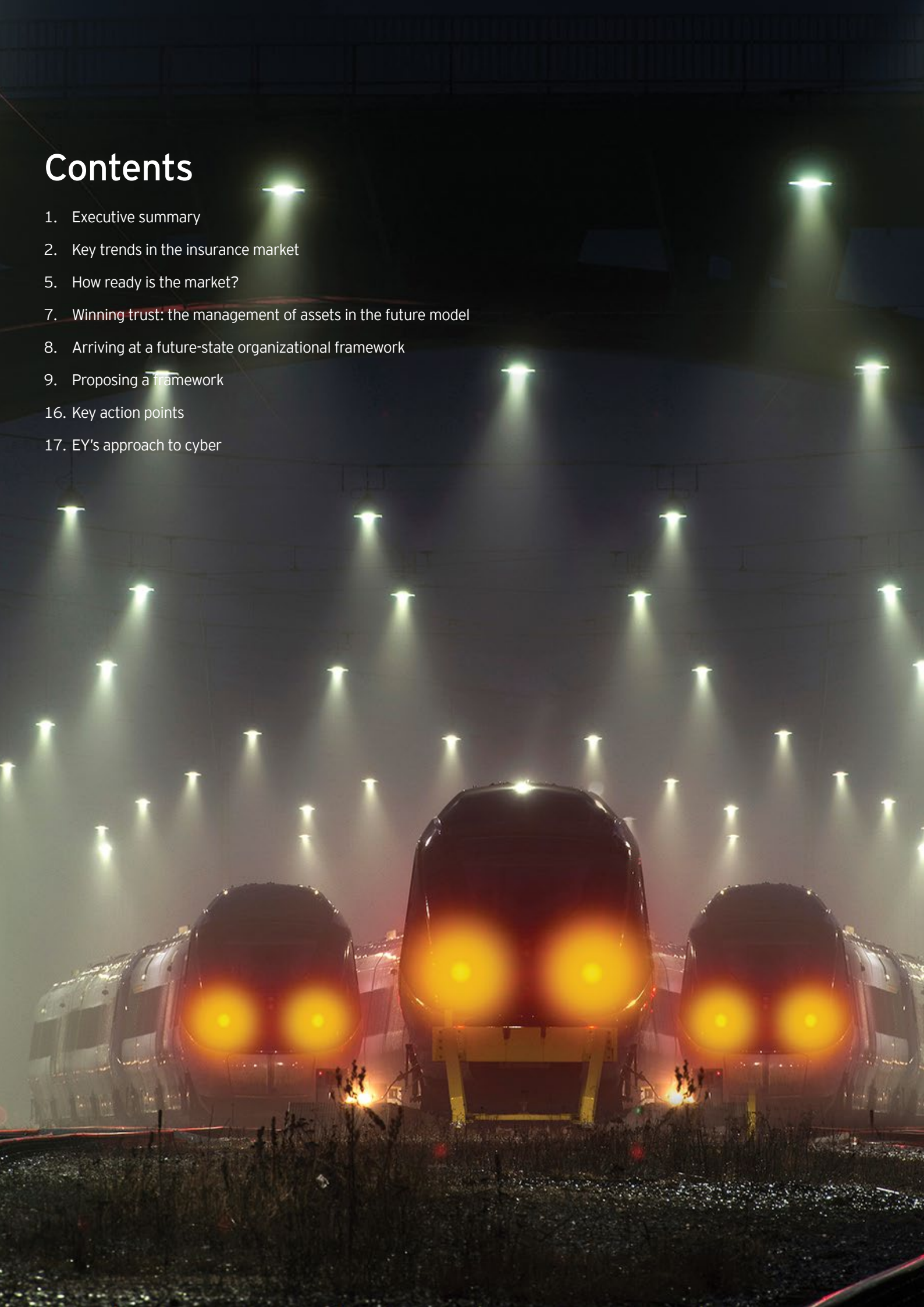
Cyber strategy for insurers

Managing physical and digital assets to protect brand and reputation

EY
Building a better working world

Contents



Executive summary

Effective cybersecurity is essential

Innovative, global technologies are disrupting the traditional infrastructure of the insurance industry. Mobile, digital, analytics and payment platforms are accelerating rapidly. The evolution is so pervasive that the C-suite is seeking new business models to enable a stronger customer-centric focus. New models will drive growth expansively across geographical, operational and technical platforms to reach customers and meet their evolving needs. This will require new capabilities, expansion into areas such as governance and cyber risk, and a shift in oversight and responsibilities across the organization.

The EY *Blockchain technology as a platform for digitalization* emphasizes the importance that insurance companies are placing on creating a secure, common infrastructure for the digital economy. It highlights the need for resilience and attribution to secure the integrity and intimacy chain between client and insurer.

In the second of our EY Innovation series, we focus on managing critical assets and the changing boundaries between client and insurer within the context of cyber risk. We predominantly focus on issues that will confront the C-suite and assess the impact on the organization, including shifting C-suite responsibilities and changes of behavior resulting from operational processes and greater use of third-party providers. We explore increasing risk exposures, and how brand and reputation can erode when insurers fail to develop an operating model framework or understand data types and flows. Any breach of the client-insurer relationship that dilutes the customer experience or, worse, causes a loss of data leads to legal disputes or regulatory fines. There is increasing pressure on insurance companies to comply with regulatory requirements and European Union security and breach regulations.

As innovation and digitization evolves, insurers need to interpret management's challenges by asking these fundamental questions:

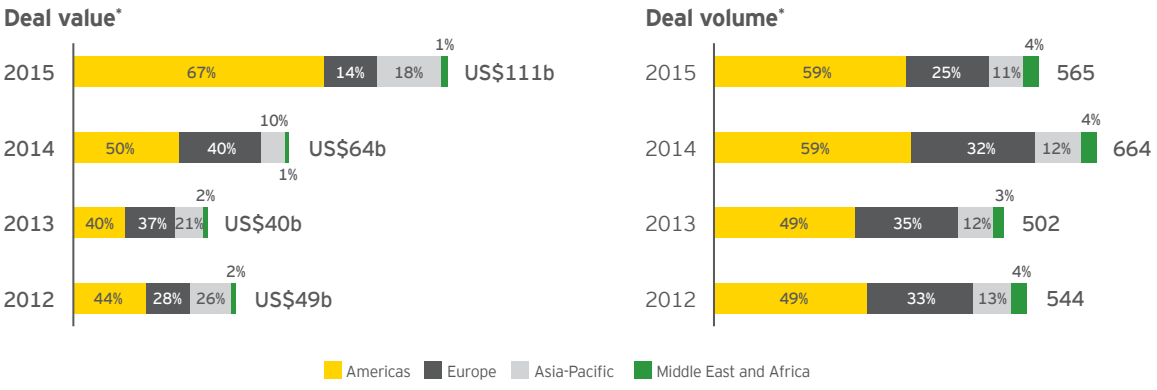
- How do you identify and protect customer assets, particularly in a world that continues to digitize?
- What are the weaknesses and sources of disruption in your operating model, particularly with respect to third parties?
- Do you understand the risk appetite and risk culture needed to protect your brand?
- What is the impact to your organization, including changes to behavior and responsibilities of the C-suite?
- What is on your compliance agenda and your response to regulatory requirements?

Optimizing a framework to respond to technological opportunities, risks and disruption will protect brand and reputation, enhance investor confidence and prepare insurers for the challenges of tomorrow.

Key trends in the insurance market

Insurance companies face many diverse risks that present opportunities and challenges. Conduct risk, data and disclosure, security around networks, cyber threats and regulatory uncertainty are foremost on the list. This comes at a time when the industry continues to cope with slower economic growth, high costs, low investment returns and market volatility. The changing landscape is leading to more complex business boundaries in the form of consolidation, innovation, disruptive technologies to support consumer demands and the increasing use of third-party agents, including digital and cross-border alliances.

Consolidation in the market model



Expansion and increased M&A activity are prevalent in the market, and reinsurers are increasing their share in direct access to domestic markets. This is coupled with a drive to consolidate existing businesses, including outsourcing and shared service centers using third parties. As global facilities in commercial and specialty markets increase, so does their use of third parties and underwriting agents. Further analysis on global insurance deal activity can be found in our report *Global insurance M&A themes 2016*.

Embracing consumerization

Technology has developed exponentially over the past ten years, leading to new emerging assets being at risk: robotics, cloud, the internet of things, augmented reality, driverless cars, medical advances and wearable technology, to name a few. Some digital agendas may include apps in which insurance companies may transact customer data or new forms of payment.

At the customer level, this opens the door for insurers to introduce or redesign insurance products — many of these will be cyber- and technology-related to address the latest trends in insurance exposures and losses. Risk managers of physical assets will now be teaming with risk managers of virtual assets, which will be a major shift for insurance organizations. Responding to cyber and data breaches will create a new way of analyzing risk, supported by processes and operational models that will be more agile in adapting to change.

As consumers continue to demand services 24/7 globally and insurance companies expand internationally across borders, insurers are developing disruptive tools to help manage the risks. These technologies include increased usage of tablets and mobile-to-mobile payments, big data analytics, aggregators, third-party contracts and personal digital devices that offer customers an unparalleled experience. Consumerization is causing a fundamental shift from a product or service offering to a more personalized, user-driven strategy that focuses on customer needs and preferences.

While access to technology for the consumer is available, the main issues for insurers are back-end processing systems, legacy technology and manual processes.

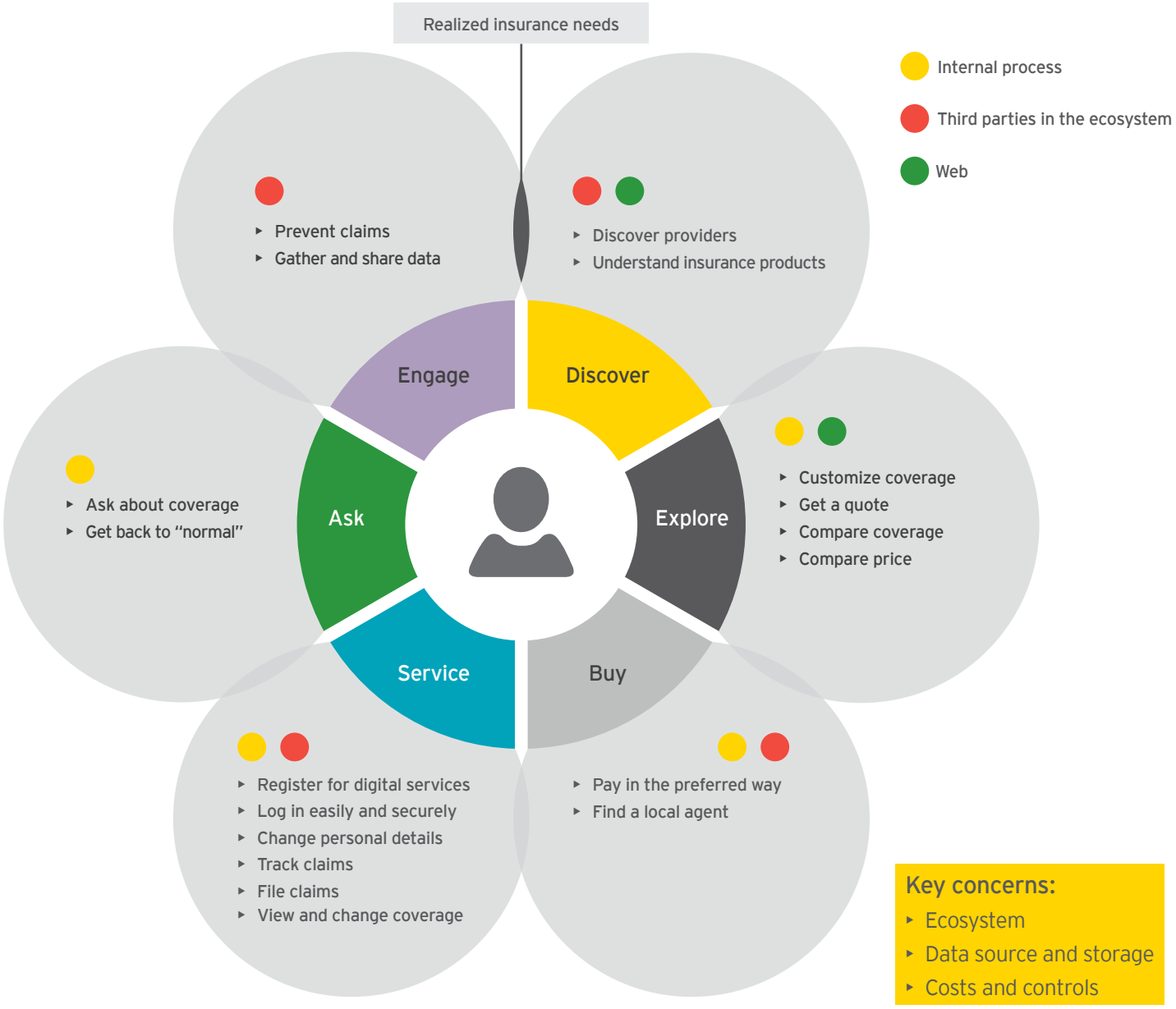
Platforms for innovation and disruption

The need to support consumers across multiple platforms and channels (e.g., the rise of InsurTech and FinTech propositions, mobile and agency networks) is leading to the creation of third-party models for technology platforms and FinTech payments. Future channels and disruptive models are emerging that are changing the insurance ecosystem and laying the groundwork for digital transformation and meeting changing customer demands.

As new platforms replace traditional ones, insurers need to rethink distribution channels, market segmentation, operational efficiencies and go-to-market strategies. Innovation continues to commoditize the value chain at a significant rate, squeezing insurers at both ends of the spectrum. Continual advances in disruptive technologies empower consumers and provide easier access to markets at one end, and industry consolidation among insurers and technology companies at the other.

At the same time, insurers have to invest in improving their internal processes and restructuring their legacy systems in order to be responsive and effective. The regulators' concern regarding these issues is the insurer's ability to control client data across the ecosystem and maintain visibility.

Mobile moments are present throughout the customer journey



Recent major cyber incidents in the insurance industry

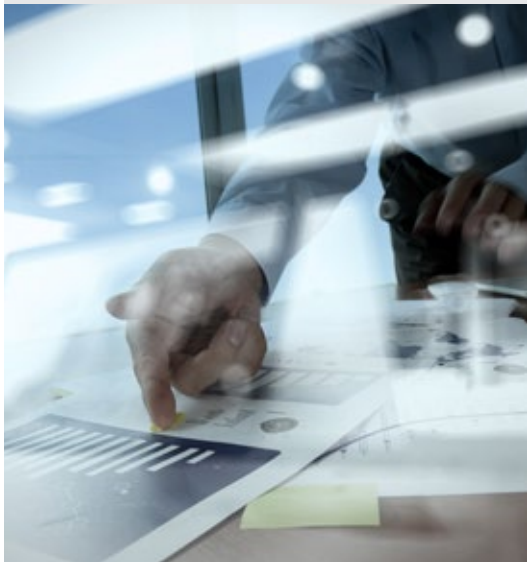
1. A US health insurer suffered an unusual cyber attack in July 2016 that compromised two separate data systems and exposed the confidential information of 3.7 million customers and health care providers. The attackers accessed both personal identifiable information (e.g., social security numbers, claims and health insurance information) and payment data, including cardholder names, card numbers and expiration dates. At least one class-action lawsuit has been filed following this data breach.
2. In 2015, one of the largest health insurers in the US experienced a cyber attack that compromised the addresses, employment information and income data of more than 78 million users. The financial consequences are expected to exceed the insurer's cybersecurity policy, which covers losses up to US$100m.
3. Another major insurer announced a data breach of their IT systems in 2015, affecting 1.1 million members. Cyber attackers acquired the members' usernames to access personal information such as names, birth dates and email addresses. The insurer notified each member impacted by the breach, and offered free credit monitoring and identify theft protection.

How ready is the market?

How ready is the market compared with our analysis?

The 19th EY Global Information Security Survey (GISS) captured the responses of 1,755 C-suite leaders, and information security and IT executives and managers, representing most of the world's largest and most recognized global companies. Key points and results of insurer respondents to the GISS provide the following data:

Market trends insurers



When asked how their information security function is focusing on the impacts of technology, 11% of insurers said they are focusing on devices connected to the internet of things; 7% are focusing on advanced machine learning or artificial intelligence; 5% are focusing on robotic process automation; and 4% are focusing on blockchain and cryptocurrencies.

Sixty-two percent say that data leakage or data loss prevention is a high priority for their organization in the next 12 months.

Fifty-nine percent of insurers say that budget constraints are the main obstacles or reasons that challenge the information security operation's contribution and value to the organization.

Fifty-five percent of insurers outsource vulnerability assessments from their information security function.

Forty percent of insurers say that end-user awareness, exploited via phishing, was the primary control or process failure leading to their organization's most significant cyber breach in the last year.

Sixty-four percent of insurers say that customers' personal, identifiable information is the most valuable information to cyber criminals.

How do insurers handle cyber incidents and losses?

Likelihood of significant attacks

49% of insurers discovered "significant" cybersecurity incidents within their organization.

Difficulty in detection

71% of insurers did not think it was very likely that their organization would be able to detect a sophisticated attack.

Constraints

59% of insurers lack executive support and view budget constraints as the main obstacle to tackling cybersecurity.

83% of insurers say that the discovery of a breach resulting in attacks on the organization is likely to encourage them to increase their information security budget within 12 months.

Quantifying the damage

19% of insurers do not know the financial impact of cybersecurity incidents on their organization – more do not know the impact of cybercrime on their key customers.

Source of attacks

56% of insurers see criminal syndicates as the most likely source of cybersecurity attacks.

82% of insurers say careless employees are the most common cause of attack. This is a significant increase from last year, when insurers did not consider threats from inside their organization likely.

Viability of current approach

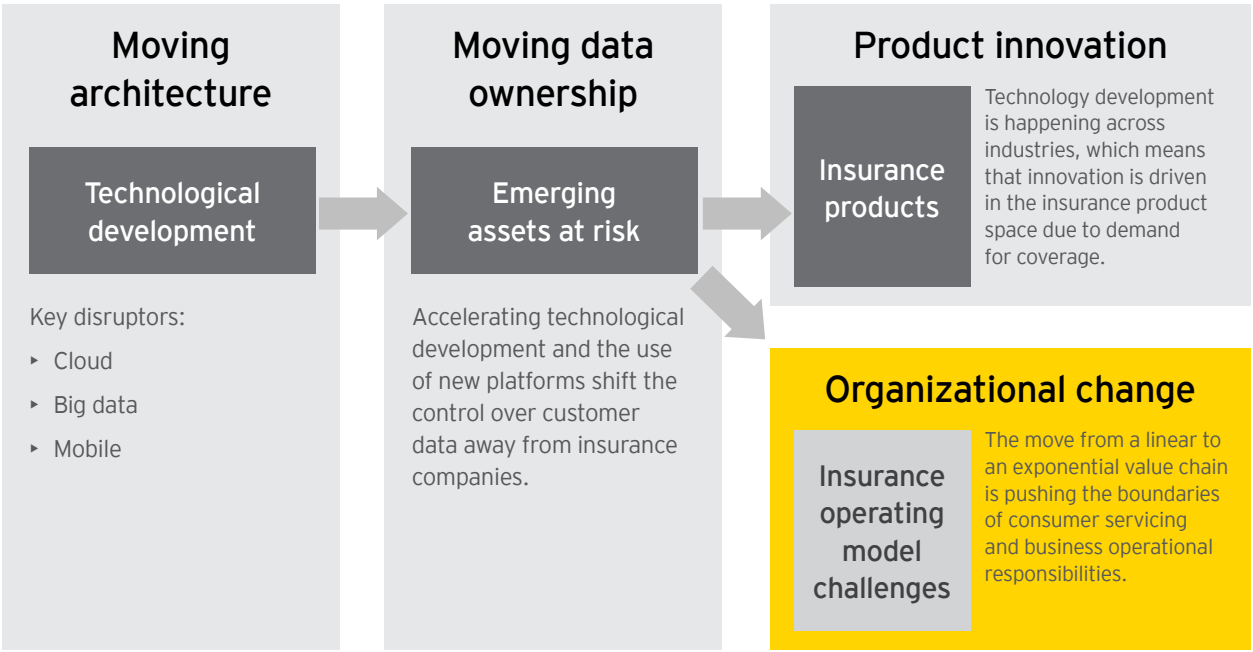
11% of insurers believe that their approach to cybersecurity is fully meeting the needs of their organization.

Winning trust: the management of assets in the future model

As innovation and digitalization drive forward, some of the most important challenges on the management agenda are the ability to understand:

- The ways in which brands can be eroded, and how to govern the boundaries of the business and critical customer information
- The changing nature of boundaries between customer and insurer
- Increasing risk exposures (including cyber threats)
- How the level of technical expertise will dramatically change the role of underwriters, claim managers, actuarial and other key functions

Fragmentation of the customer value chain brings challenges to the ability to control the fragmentation



Arriving at a future-state organizational framework

As these themes emerge, insurers tend to look immediately at the risks and threats to their business. The proposition is that they should think about a framework — an operating model that uses values, critical assets and outsourced arrangements. In addition to assessing the risks, they need to review the risk culture and cyber risk appetite while considering compliance issues surrounding cyber-related governance practices.

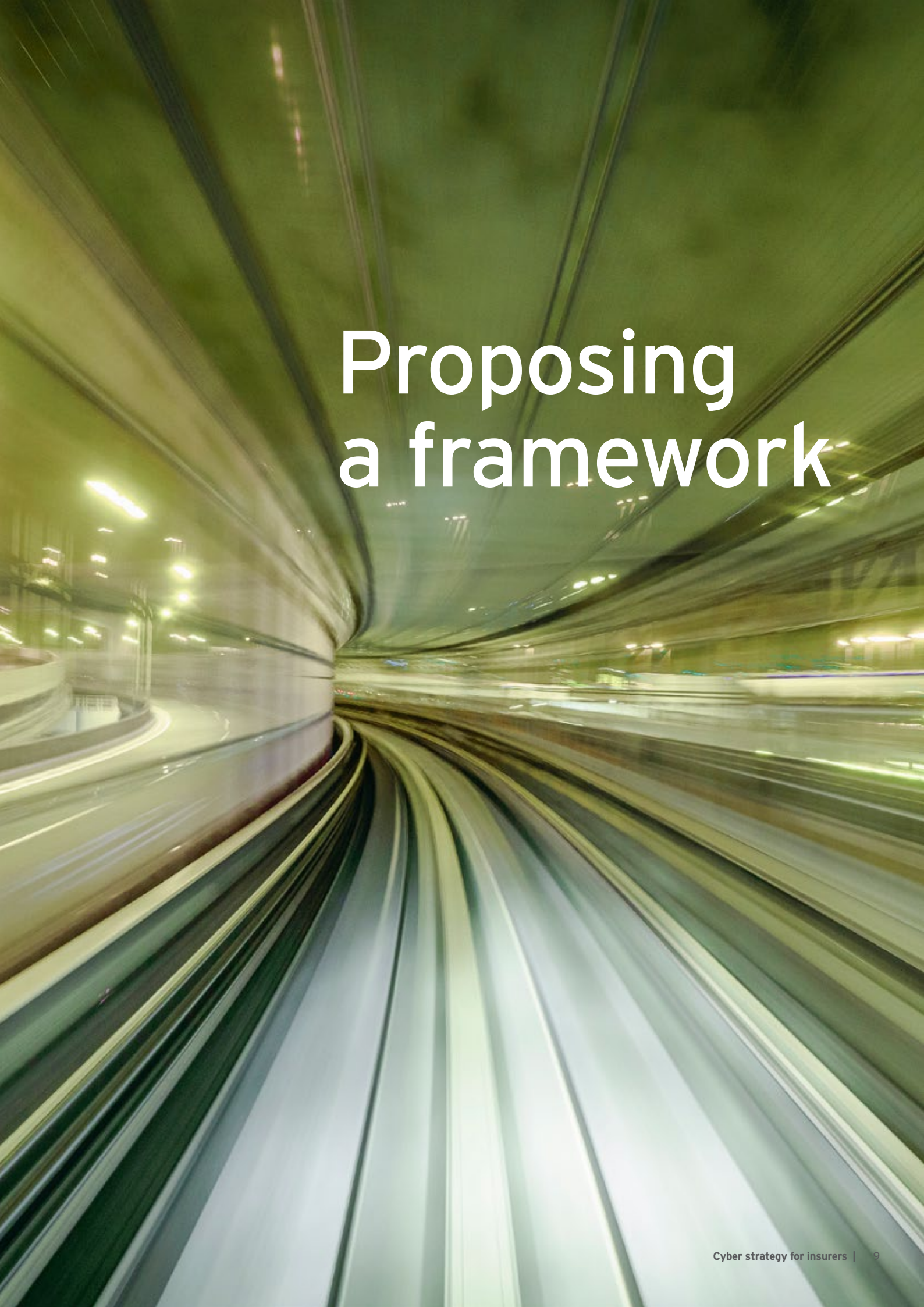
In terms of a future-state organizational framework, we suggest considering the following points:

1. Operating model and culture
2. Process and assets
3. Roles within the organization
4. Investment in proactive security

Relationship of questions to framework or approach

In order to understand the readiness of their organization and business implications, insurers need to ask these key questions:

1. Do you understand what your assets are and the trust agenda? How do you protect customer assets across different channels, processes and levels of sophistication and maturity? What controls are in place to provide the required transparency and reporting?
2. Do you recognize weaknesses and sources of disruption in the model: response, service, trust, quality, capital, security and relevance? If you do not know you have been hacked, how do you reassure your investors that they are protected?
3. What is your risk appetite and risk culture? How are responsibilities changing? Is the CEO protecting the brand, or the CIO or CTO?



Proposing a framework

1. Assets

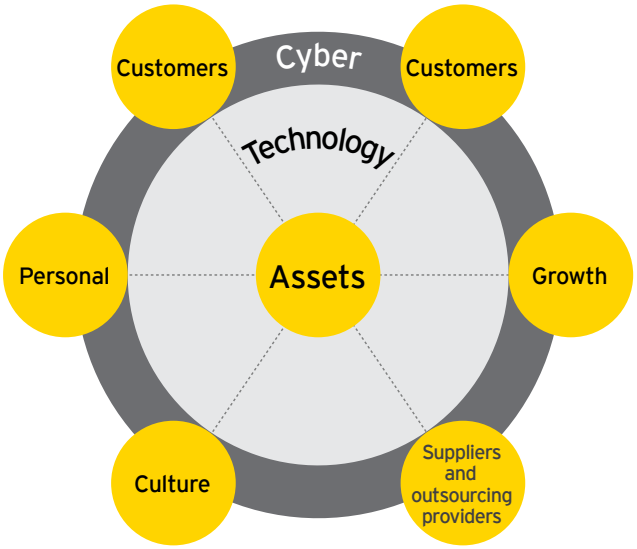
Identifying critical assets

Identifying the critical assets that are likely to be targeted, creating a list, monitoring and gathering information is key. Assets of value can be in different forms (e.g., people, data, infrastructure and relationships), and not all data is equal. Insurers need to define what is of interest to attackers, the location of assets, accessibility and the detection time frame. This may include board reports, customer data, M&A information, batch files, cryptographic keys, passwords or other credentials, as well as the impact of business plans on asset vulnerability. Risk appetite needs to link to business decisions, security requirements and critical assets. Using a top-down and bottom-up approach provides a mechanism to prioritize allocation of resources.

Defining assets within the business

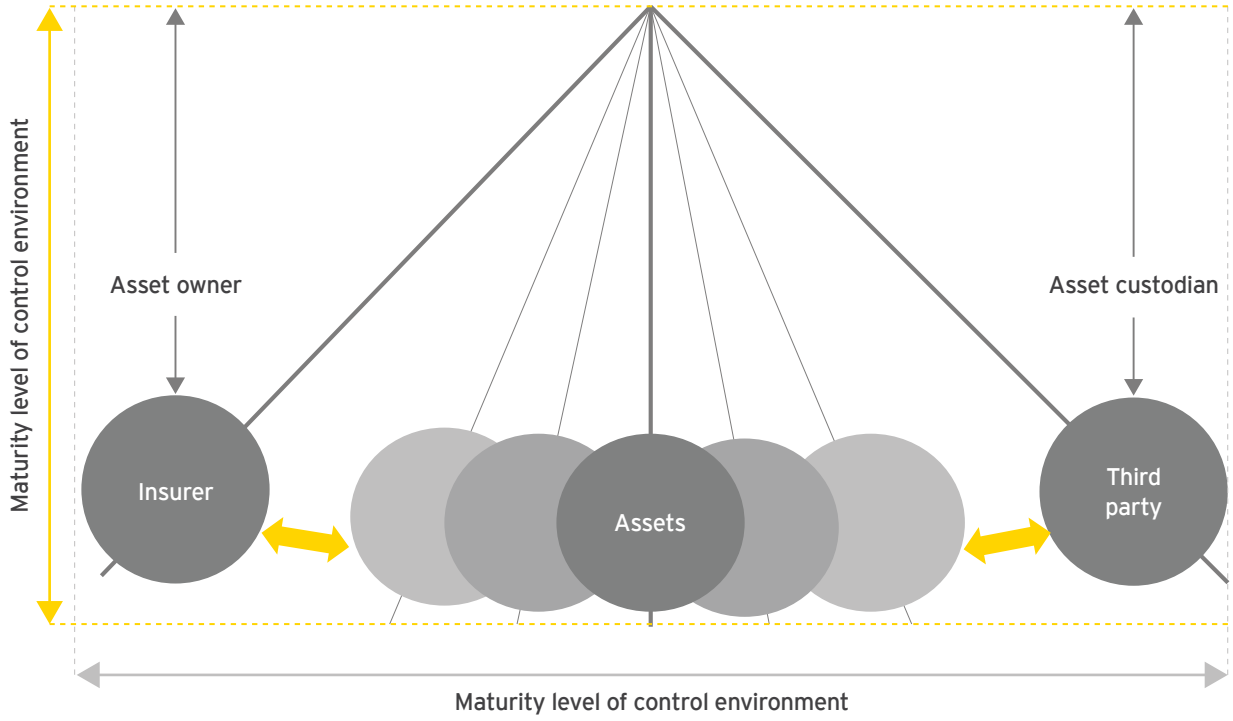
Insurers need to define their assets to leadership throughout the organization. These assets are influenced by cybersecurity and technological advances, and should be viewed within the context of customer, culture and risk awareness relationships. A business plan influences the decisions — and the wrong channels could deter opportunities. Organizational assets such as customers, culture, and suppliers and outsourcing providers influence the business processes and transpose the technology environment and security challenges.

Operational processes within insurance companies are digitized, as are insurers' assets. Most insurers will need to take a radical approach to transform their operations, use the latest innovative capabilities, and reduce core demand from both internal teams and external customers. An innovative insurance company will embrace InsurTechs and industry disruptors such as robotic automation, analytics and artificial intelligence, and look to other industries for new partnerships and ideas. Insurers will need to rationalize the factors driving complexity (i.e., channels, products and locations), streamline management processes and speed up decision-making. Sustainable value and an agile business environment can be achieved by establishing a target operating model and road map that aligns with strategy, and embracing a flexible portfolio approach. This simplification and digitization of the insurance operating model brings with it inherent consequences for the ownership and control of assets.



Understanding assets in outsourced arrangements

The custody of assets previously managed by an insurance company may shift under leaner operating models (outsourcing agreements). This implies a loss of control over the assets by the outsourcing company to a third-party provider. While establishing a more agile digital supply and processing network provides operational efficiencies, there is greater risk of losing control over critical assets. Even if parts of the operation are outsourced, the risk to the outsourcing company remains, while the responsibilities shift to third parties. The increased controls in managing in-house and third-party providers impacts the organization and the value proposition.



2. Operating model and culture

Operating model

A lean operating model with simplified and enhanced systems decreases the risk to business operations and inefficiencies stemming from legacy systems, and it adapts to changing market conditions and future technological change. This operating model must be aligned for the digital world to drive agility and innovation, redesign the organization to fit the digital age, and leverage new technologies to enhance operations.

Review risk appetite statement

The board must make intelligent decisions on what risks can be taken, and the cyber risk appetite must accept the new reality. Concepts such as "leading practice" or "most secure" for any large financial services organization today are unsustainable and cannot be implemented. The cyber risk appetite must be aligned with the overall business strategy, risk appetite and tolerance. It must set the tone for the organization, and enable the right investment and decision-making. Cyber capabilities come at a cost to the business, requiring the right resources, focus, processes, technologies and investment. The value of the cyber risk appetite is the cyber strategy built on it. It enables an insurer to remain competitive; protects assets, brand and reputation; enhances user experience; and, most importantly, enables innovation.

Risk culture

Insurers need to implement processes to drive the adoption of leading practices and enterprise-wide acceptance of cyber risk culture. Risk culture should include a positive message and frequent company-wide training at all levels, including the C-suite. A real corporate culture of awareness and leading practice will set the organization apart and enable an adequate level of preparedness and responsiveness. Employees remain an important asset to insurance organizations and should be protected from outside exposures, encouraged to act prudently, and be comfortable to report risks and assist in reducing insider threats. Insurers need to minimize the silo approach in order to increase interaction between functions and improve the flow of information. They need an integrated risk management culture and processes, created by a diverse culture of innovation that uses digital technologies to empower the team.

Compliance

Government and regulatory bodies are driving cyber-related governance practices around the collection, storage and use of data. Compliance with data protection laws, pro-privacy bills, cybersecurity and information sharing will require significant investment. Insurers will need to adopt written cybersecurity policies and procedures on customer data privacy, service providers and network security — or face heavy fines for non-compliance. Responding to regulatory challenges will enable innovation, improve governance and encourage a more effective approach to cyber risk management.

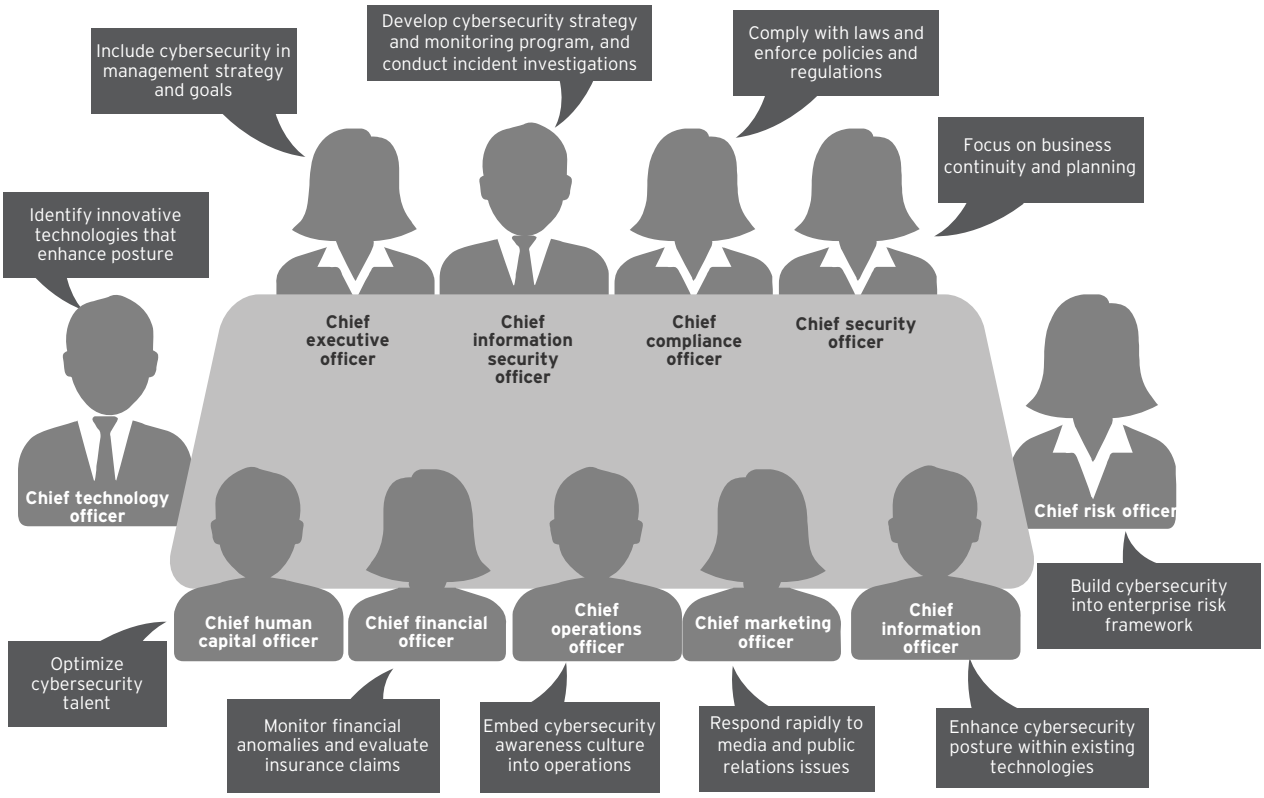
3. Readiness of the insurer and roles

Impact for the C-suite

Due to the shifts in operational processes and the increased use of third-party providers, there are challenges for the C-suite around their role, definition of priorities and impact. They have to manage the changing nature of third-party contracts to deal with cyber and data controls or assumption of risk. The establishment of a chief listening officer with changing ownership and relationship models could be on the table. There are changes to the responsibilities in terms of the transition away from CIO ownership of risk to the CEO or CRO, and the impact on people in the business and their management.

Embed cybersecurity across the C-suite roles, and beyond, to protect your most critical assets

The C-suite should be fully embedded within the organization and operating model, with clearly defined roles and responsibilities. In doing so, leadership should effectively answer important cybersecurity questions, both proactively and should a breach occur.



Cybersecurity and the board

As cyber risk is abundant within the digital age, it is essential for the board to have cybersecurity as a priority on its agenda and embed major discussions and decisions on cyber risk continually at board meetings. The board is responsible for understanding the risks to the organization, defining cybersecurity governance and setting the expectations for management. Cybersecurity is an organization-wide risk that should be managed by the board on an ongoing basis through assessments of current cybersecurity practices.

Not only does the board maintain responsibility for cybersecurity, it is also responsible for planning for cyber risk and rehearsing the response within the organization. This is essential for preparing management and all personnel for an event that may occur.

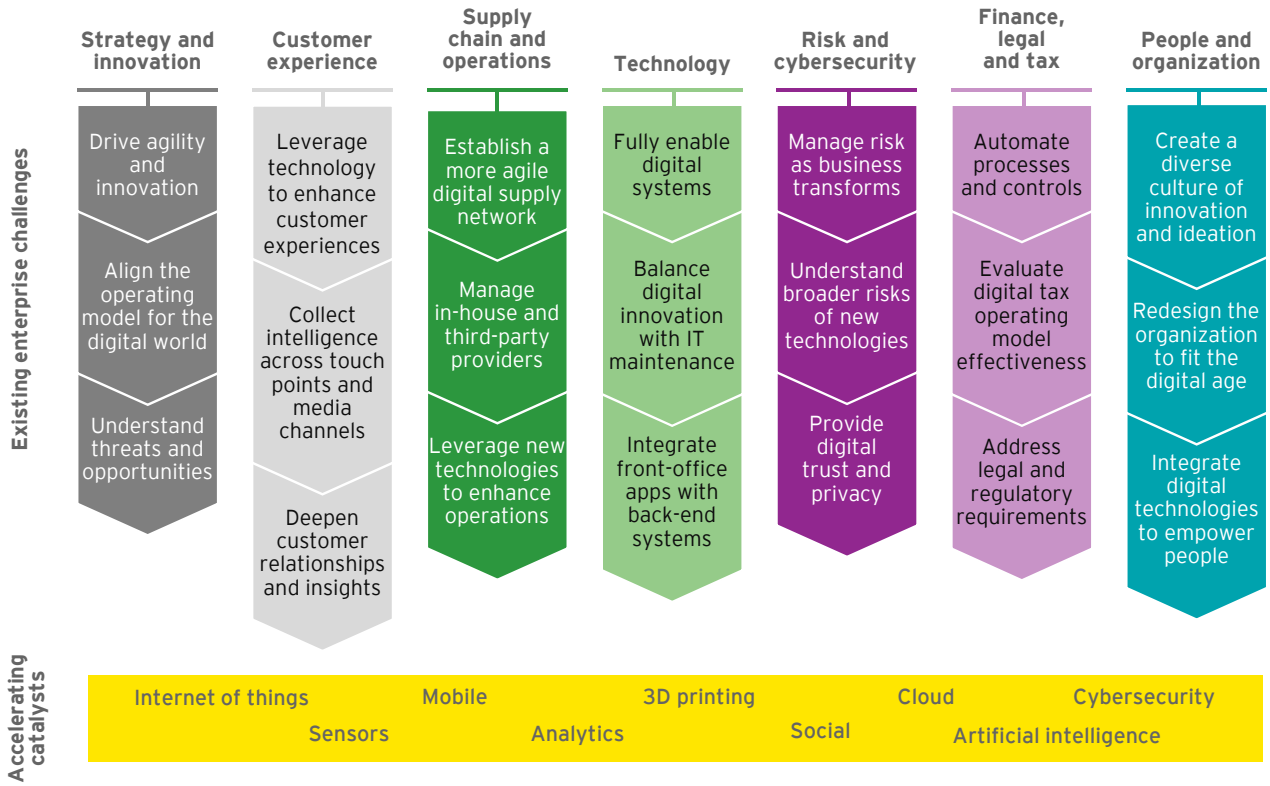
4. Investment in proactive security

Risk assessment

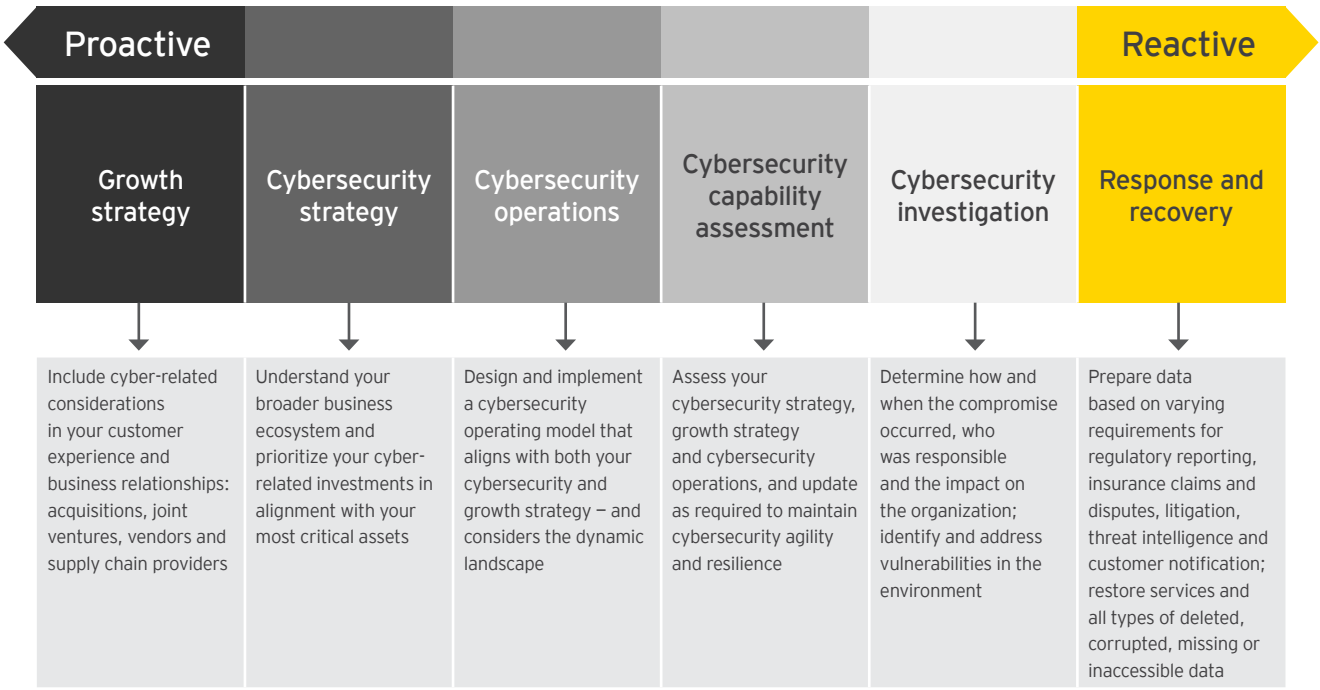
It is essential to understand data types and flows, criticality of a network or system, business continuity processes, brand considerations, key people and third-party dependencies. Organizations need to manage risk as business transforms, understand the broader risks of new technologies, and provide digital trust and privacy. The type of business model and consequential ability to react to incidents is an essential component in the risk assessment process. The use of external service providers to review risk practices and exposures is the best approach to monitor controls and present a holistic view of the risk landscape.

Powered by big data and advanced technology, digital is disrupting everything from business models to entire industries; therefore, it needs to be assessed to determine the impact to the business now and tomorrow. A digital enterprise has the agility and innovation DNA to exploit digital technologies and data across every facet of its business, at the cadence of the new digital economy, to gain adaptive advantage.

The risk assessment process should aim to evaluate new technology and digital risks, such as expanding threats, rapid change, rising costs, and global and technical connection across the digital enterprise.



The chart below shows how organizations should embed cybersecurity within their operating model to manage risks proactively and reactively.



Key action points

In looking to ensure that the cyber risk appetite is sufficiently comprehensive, insurance companies should incorporate the wider risk, control and governance frameworks operating within the business.

Cybersecurity should be a standing boardroom topic:

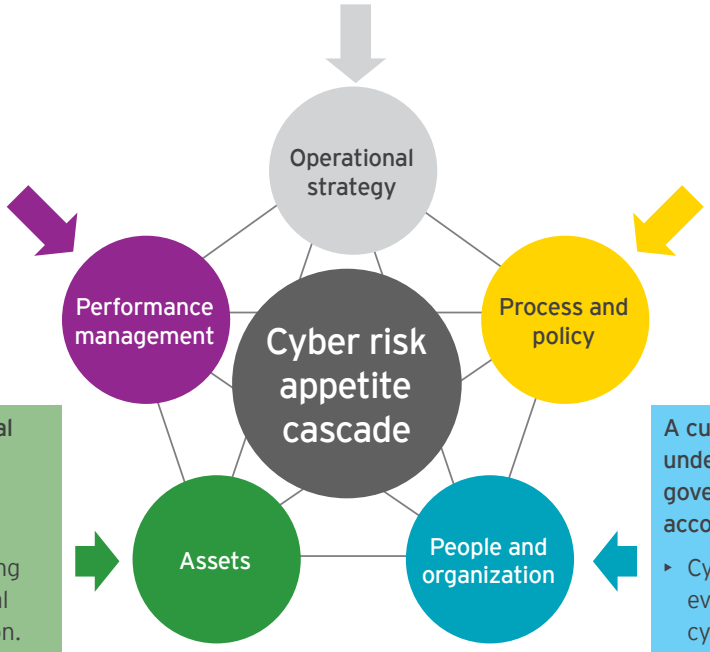
- Risk appetite should enable leadership to understand, monitor and discuss how cybersecurity helps the business to innovate and manage risk.

Readiness to deal with cyber attacks requires behaviors that are thoughtful, considered and collaborative:

- Risk appetite should be linked with performance management and remuneration to ensure that desired behaviors are incentivized and rewarded.

Risk assessments should enable an understanding of exposures and identify levels of risk:

- Focus on assets, external interdependencies, threat vulnerabilities, controls and testing activities.
- Regularly stress test appetite via rehearsal of incident response capabilities.



Understand the most vital informational assets and their value:

- Risk appetite should reflect this by prioritizing the protection of critical systems and information.

A culture where everyone understands the need for strong governance, user controls and accountability for cyber risk:

- Cyber threats are constantly evolving, and risk appetite for cyber risk should drive change.
- Appetite should extend to cover the firm's broader network, including suppliers.

Insurers can protect their businesses, reputation and responsiveness by creating an agile environment. Recognizing the importance of governing critical information about their clients – their assets, risk requirements and preferences – is critical to retaining business. They also need to understand the link to unlocking cost advantages and innovation, free from the constraints of legacy systems. To create an agile environment, it is necessary to identify critical assets and build a framework to realize opportunities.

Optimizing the operating model and framework in response to technological opportunities, risks and disruption will prepare your business to conduct itself with agility. The positive results include safer, responsive businesses that increase and maintain investor confidence and are prepared for tomorrow.

The key issues are around organizations knowing their assets, obligations of senior management in the face of the changing regulation, and the need for insurers to understand and embrace the increasing sophistication of online and other channels. Finally, organizations must define roles and responsibilities, as some duties may shift from the CIO or CTO to the CEO.

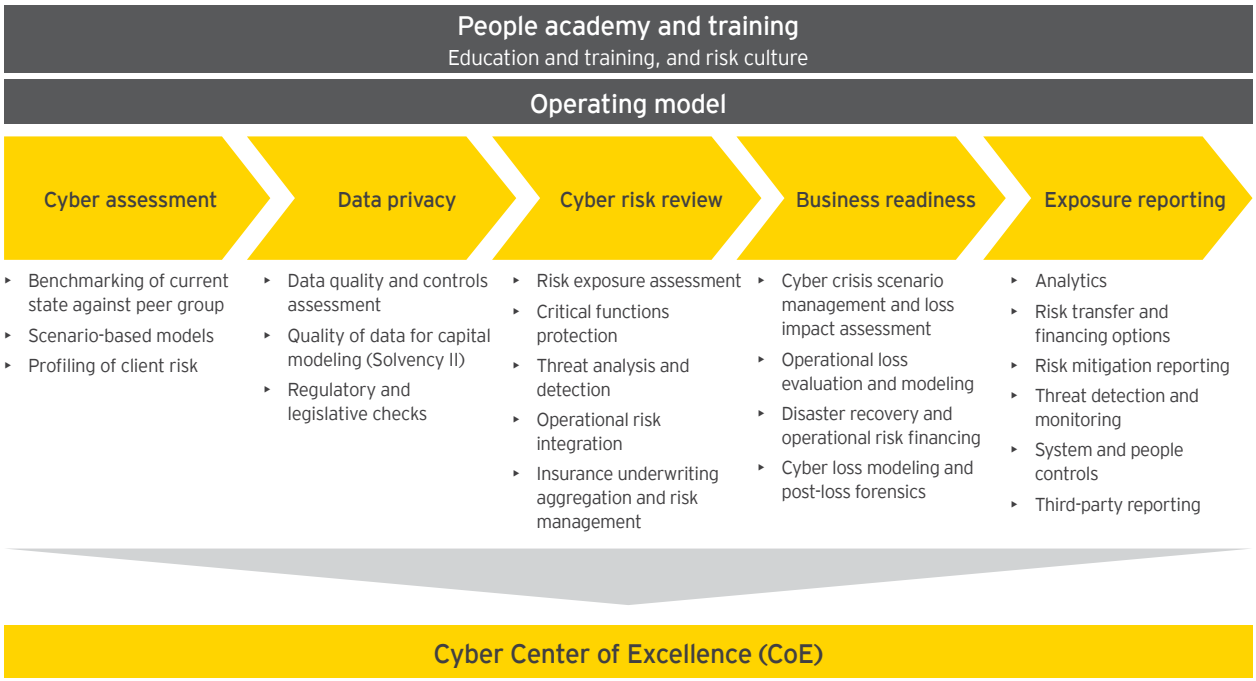
Most insurers are early in the process of developing a cyber strategy for their businesses. EY can helps clients understand:

- How to define and prioritize assets in their organizations
- The differences in customer assets across channels, processes, levels of sophistication and maturity protected
- How to deploy responsibilities across the C-suite and cascade the risk culture throughout the organization

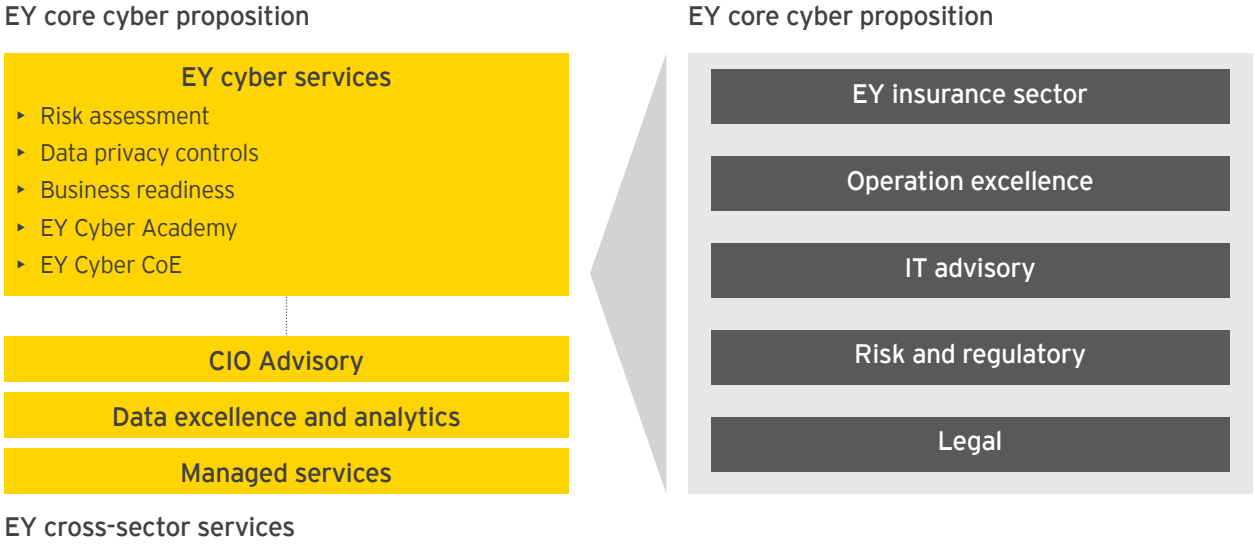
EY's approach to cyber

EY offers a number of services to help our clients understand and react to the changing world of cyber threats, depending on their levels of risk appetite and internal capabilities.

EY's approach to cybersecurity focuses on the following areas:



We understand the commercial priorities and imperatives of our clients and their customers, and the challenges insurers face from evolving threats and regulations. Our professionals provide cyber services with a holistic understanding of operating models, processes and capital.



EY contacts:

Shaun Crawford
Global Insurance Leader
+44 20 7951 2172
scrawford2@uk.ey.com

Cheryl Martin
Global Insurance Cyber Leader
+44 20 7951 8742
cmartin@uk.ey.com

Contributors:

Ian Meadows
+44 20 7951 9594
imeadows@uk.ey.com

Alexandra Schedat
+44 20 7951 1881
aschedat@uk.ey.com

Luca Russignan
+44 20 7980 9635
lrussignan@uk.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no: 00060-174Gbl
CSG no: 1606-1964995 NE
ED None

ey.com