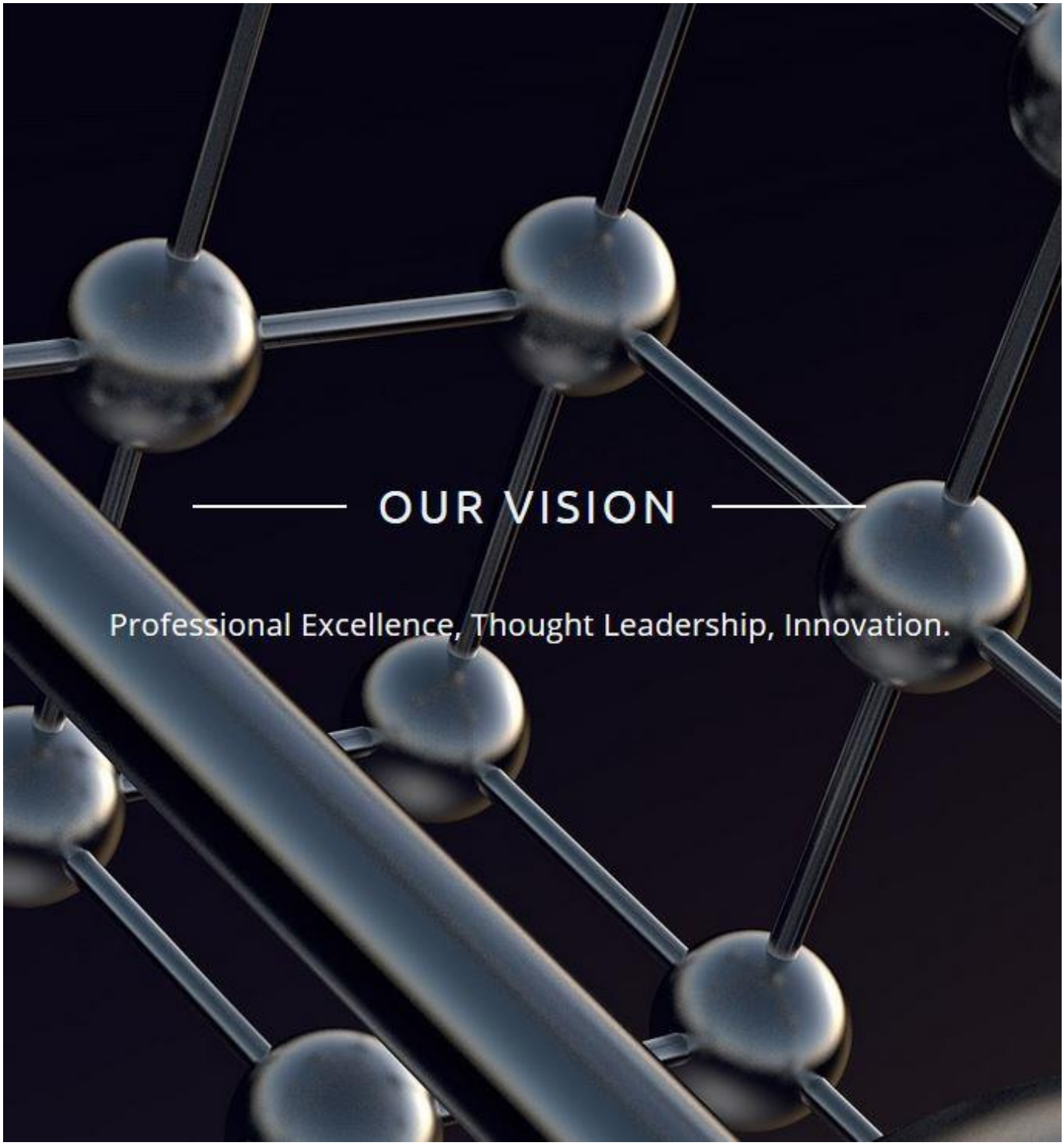
Risk Management News – April 2017



Using Catastrophe Modelling to Predict Risk

Modeling pushes insurers to consider the potential outcomes for low probability, high severity events. (Photo: Shutterstock)

The insurance industry has been using statistical models to provide guidance towards data-driven decision-making for many years.

Life insurance companies have mortality tables going back a century or more, allowing actuaries to determine rates for today's life insurance customers that will maintain future profitability while fulfilling the promises made in the policies.

The explosion of computer technology in the last 50 years has created opportunities for data gathering and analysis that could only be dreamed of even a generation ago. Insurers now have the ability to sift through mountains of data to help derive useful insights and estimate the potential impact of a variety of possible future events.

Massive Fire at US Sheet Metal Plant After Explosion

Heavy flames and plumes of black smoke could be seen for miles Monday as firefighters battled a massive, explosive fire at a Montgomery County sheet metal plant.

The five-alarm fire began at Trico Metal Products, a sheet metal fabricator business on the 2300 block of Wyandotte Road in Upper Moreland around 5:20 p.m. Officials said there were reports of an explosion prior to the blaze.

Partial Collapse at Sheet Metal Plant After Fire

Part of a sheet metal plant collapsed during a massive fire.
(Published Monday, March 2, 2015)

A front wall and back wall of the facility collapsed as numerous explosions from overheated compressed gas cylinders inside the plant put responding firefighters at risk.

"There are no hazardous materials or anything that affected the community," said Willow Grove Fire Chief Brian Focht. "However, as a danger to firefighters there were multiple explosions and a building collapse."

Insurance Implications of Legal Marijuana

Because businesses in the marijuana industry face unique challenges, yet have all of the traditional insurance needs, insurers are still working out coverage questions. (Photo: Shutterstock)

Even before the first wisp of legalized recreational marijuana smoke hit the air nearly five years ago, there were many questions regarding what ramifications this drug would have on the insurance industry.

Today, with more than half of the states decriminalizing or legalizing the use of marijuana for recreational or medical use, questions still abound.

Coverage questions

Although some insurers have been cautious in offering coverage to businesses involved in the multi-billion-dollar marijuana industry, others have seen this as a niche opportunity. Because businesses in the marijuana industry face unique challenges, yet have all of the traditional insurance needs, insurers are still working out coverage questions.

For example, product liability issues could come into question for a retailer selling a food product that contains marijuana. Not to mention the challenges of an all-cash business and the questions regarding exposure to armed robbery.

For non-marijuana businesses, there may be property insurance questions regarding the exposure to vandalism, fire and mold, particularly for a business moving in adjacent to where marijuana is being grown. Local businesses may face additional liability exposures from patrons who are high injuring other customers.

Legalized marijuana has also raised issues dealing with an employer's ability to maintain a safe and drug-free workplace. For example, there could be employment practices liability concerns for employers that have workplaces with heightened safety concerns and stringent enforcement of a drug-free environment because employees are operating machinery or driving vehicles.

Identity Theft Used To Scam Insurer Out Of 2500 Cell Phones

NASHVILLE, Tenn. — US Federal prosecutors say a man who scammed his way into getting an insurance company to ship out nearly 2,500 fraudulently obtained cellphones has been sentenced to serve more than five years in prison.

Acting U.S. Attorney Jack Smith of the Middle District of Tennessee said 24-year-old Johnny Santiago Valdez Calderon was sentenced to serve 61 months in prison for engaging in a wire fraud and identity theft scheme.

Court documents say Valdez Calderon was living in the Dominican Republic but having runners pick up phones shipped to hotels around the U.S., sell them and send him most of the proceeds.

Officials say Valdez Calderon assumed the identities of the Nashville-based insurance company's customers to submit fraudulent claims online. It's not clear yet how he got the customer's identity information.

This again shows the need for strong data security and Cyber Insurance to protect businesses against data loss ad liability for third party client losses.

Insurer Uses Drones to Assess Storm Damage

The insurer is using the technology to get a better idea of the property damage situation from spring storms.

Allstate is using insurance drones to conduct an assessment of the property damage left behind by spring storms in four states. The company already owns the technology in a number of locations and was prepared to implement it when it was needed.

In preparation to use the drones, Allstate Insurance readied itself with a solid fleet of the technology.

The Allstate fleet of insurance drones are either ready or already being deployed in Oklahoma, Texas, Colorado and New Mexico. These machines help adjusters to view and evaluate the extent and details of damage left behind by spring storms.

This spring's storm damage evaluation represents the largest drone launch Allstate has ever used. It is also being seen as a sign of things to come in terms of the way insurance claims will be assessed throughout the industry. If this is true, it would mean that Allstate is leading the way with state of the art aerial imagery when it comes to insurance property damage assessment.

Allstate has been researching the use of insurance drones for over two years for use like this.

Emerging Technological Influences on Liability Risk

As technology is infused at greater speeds into the insurance industry, an increasing number of liabilities, such as autonomous driving and 3D printing, will rise as result. (Source: Shutterstock)

Technology's influence on the insurance industry continues to grow in the age of digitalization. As the industry continues to infuse technology into its practice, it is increasingly susceptible to technological liabilities, such as increasing cyber and product liabilities and recall risks.

Business models in the digital economy are more complex and without clear borders, making liability harder to apportion and claims more complex to settle — despite the frequency of claims expected to decline. The growing "sharing economy" raises new questions about liability. In the future, a road traffic accident could involve the vehicle manufacturer, software provider, and the fleet operator, as well as third parties involved in the accident.

Allianz's Global Claims Review report, which focuses on global developments in liability-related insurance over the period 2011 to 2016, examines which future influences will impact liability claims going forward.

More liabilities for the automotive industry

The rise of autonomous driving will have a number of implications for insurers. Autonomous driving suffered setbacks in Arizona after a high-impact crash involving one of Uber's self-driving SUVs.

Printing up fresh liabilities

Manufacturing continues to search for faster and cheaper production possibilities. 3D printing provides such revolutionary feasibility. The technology is now widely used, especially for creating prototypes and bespoke parts in industries like aviation, automotive and the medical sector.

This will have a number of potential implications for insurance. While 3D printing could play a positive role in addressing rising business interruption exposures, it could also make it harder to trace products through the supply chain.

AIG Taps into Consumer Fears with New Cybersecurity Product

American International Group Inc (AIG.N) is joining insurers offering products that offer consumers safeguards against hackers and cyber criminals who might steal personal data.

The U.S. insurer plans to roll out a product on Monday that offers coverage for expenses that arise from online bullying, extortion and other digital misdeeds. Called "Family CyberEdge," it includes public relations and legal services, as well as at-home assessments of family electronic devices, executives said in an interview.

Wealthy, high-profile individuals have increasingly become hacker targets, said Jerry Hourihan, president of AIG Private Client Group for the United States and Canada. Social media use and online financial information make them vulnerable.

AIG's product follows cyber offerings from rivals, along with services from credit-monitoring firms and companies like Reputation.com – a trend that is poised to accelerate as people share more information online, analysts said.

Consumers now share loads of personal data on websites and apps and store photos and sensitive information in cloud platforms.

At the same time, high-profile hacking attacks have drawn global attention to the seriousness of cyber threats. Yahoo Inc (YHOO.O), Target Corp (TGT.N) and the U.S. government have been targets of sophisticated data heists, as have celebrities like Leslie Jones and Jennifer Lawrence, whose nude photos were hacked and leaked.

The U.S. government is poised to undo some privacy protections. Congress last week voted to allow internet service providers like Verizon Communications Inc (VZ.N) and AT&T Inc (T.N) to sell consumers' search data.

"Whenever you see a lot of news about something that is a risk, you usually see insurance companies trying to jump on that," said Robert Hunter, director of insurance for the Consumer Federation of America.

AIG's product came after customers asked for protection, Hourihan said. His unit caters to very wealthy individuals and typically insures assets like wine collections and fine art.

Texas Car Dealership's Entire Inventory Damaged by Hail

McKINNEY (CBS11) – If you think it's a pain talking to insurance agents about hail damage, try making the call to report about 1,000 cars. That's the case for one North Texas car dealer whose entire inventory came under fire from the recent storm.

A large white tent is the final stop for every vehicle on the lot at Pat Lobb Toyota of McKinney after going through a detailed inspection.

There were only a few with so much damage they didn't make it, but the owner here is determined to restore most of them to their original condition.

If your own hail-damaged vehicle has got you down, this makeshift doctor's office for dents and the technicians at work want to give you hope.

"I've had people give me a hug before. They were so happy," repair technician William Moothart said.

After hail rained down on virtually every one of the thousand vehicles on his lot, owner Pat Lobb may have been the one who needed a hug.

"God has a sense of humor, and I haven't figured it out just yet, but we'll get through this," Lobb said.

All week, Lobb and his employees have created an assembly line at the lot's carwash for each damaged vehicle to get a complete diagnosis. After that, it's on to the other side of the lot where technicians gently pound out each dent.

"You know what's amazing is I looked at a car the other day here that had… One car had like 60 or 70 dents in it, and the car right beside it had like four. How did that happen?" Lobb said.

Customers who were waiting to pick up cars they had already bought had the option to order a new one, are now waiting for restoration and get a discount of up to a couple thousand dollars, or take the car as is with an even bigger discount.

Lobb said once the unsold vehicles are restored to factory condition, they will still sell at a substantial discount. Now with more storms on the way, the owner says he's ready for anything.

"We've already had them all damaged, what else could happen, locusts? I'm not sure," Lobb said.

Explore the value that digitalization can bring to specific markets or products

Digital transformation for an insurer is a multiyear, group endeavor. (Photo: iStock)

The traditional insurance business model, which has been resilient for over 350 years, is now being challenged by technological and behavioral change.

In the not-so-distant future, driverless vehicles may diminish or eliminate road accidents and injuries. Connected homes could significantly reduce residential hazards. The sharing economy will likely offer peer to peer coverage.

It follows that the type of consumer served by traditional insurance companies is rapidly ceasing to exist. Today's modern customers are connected and social. They are fast to switch between providers, and expect instant reward and feedback.

The insurance industry will soon find that the only way to attract and retain customers is in their very own personally digital way. With that in mind, here, in descending order, are some practices that I believe are essential for successful digital transformation of an insurance company.

Related: Embrace the shift! Transforming the insurance industry from the outside-in

No. 8: Stay focused on digital transformation goals.

What does it mean to become a digital insurer? Well, we know what it is not. It is not moving insurance products online. In fact, it is not so much to do with products at all. Customer mentality is shifting toward consuming on-demand services, such as insurance for exactly six days of a skiing holiday or coverage for a favorite custom mountain bike. To become a digital insurer is to redefine the vision in terms of the kind of service, experience and a relationship the company is able to offer consumers. A single interaction/touchpoint mindset (selling a policy and

hoping that nothing will happen) must become a relationship mentality. The value proposition should evolve from simple indemnity to prevention, education and continuous support.

Related: Insurance in the Digital Age: 3 steps to maximizing your strategy

This new kind of customer requires next generation services. Insurance offerings have to become simpler and easier to understand. Insurance companies have to enable consumers to manage services easily, give their offerings a flexible and modular structure so customers can construct their own policies, and then interact with those products by trying them out, changing them or terminating them as needed.

Customers want companies to know them, recognize them, predict their present and future needs and expectations, and see truly personalized value propositions — all while being offered a consistent, omni-channel user experience.

A successful digital plan should permeate an insurer's entire operation. (Photo: iStock)

No. 7: Aim for organization-wide transformation.

In order for digital to achieve the goal of true customer centricity and personalization, it should permeate the whole enterprise, from culture and strategy to operations, from front-end to back-end processes, from policy purchase to claims, and from finance to HR (human resources). Moreover, customers are not the only beneficiaries of the digital way of doing business. Digital also has an important role to play in making the middle office agile enough to adapt to the evolving business model and in making the back office transparent and efficient.

Related: 8 ways that digital innovation is reinventing insurance customer service

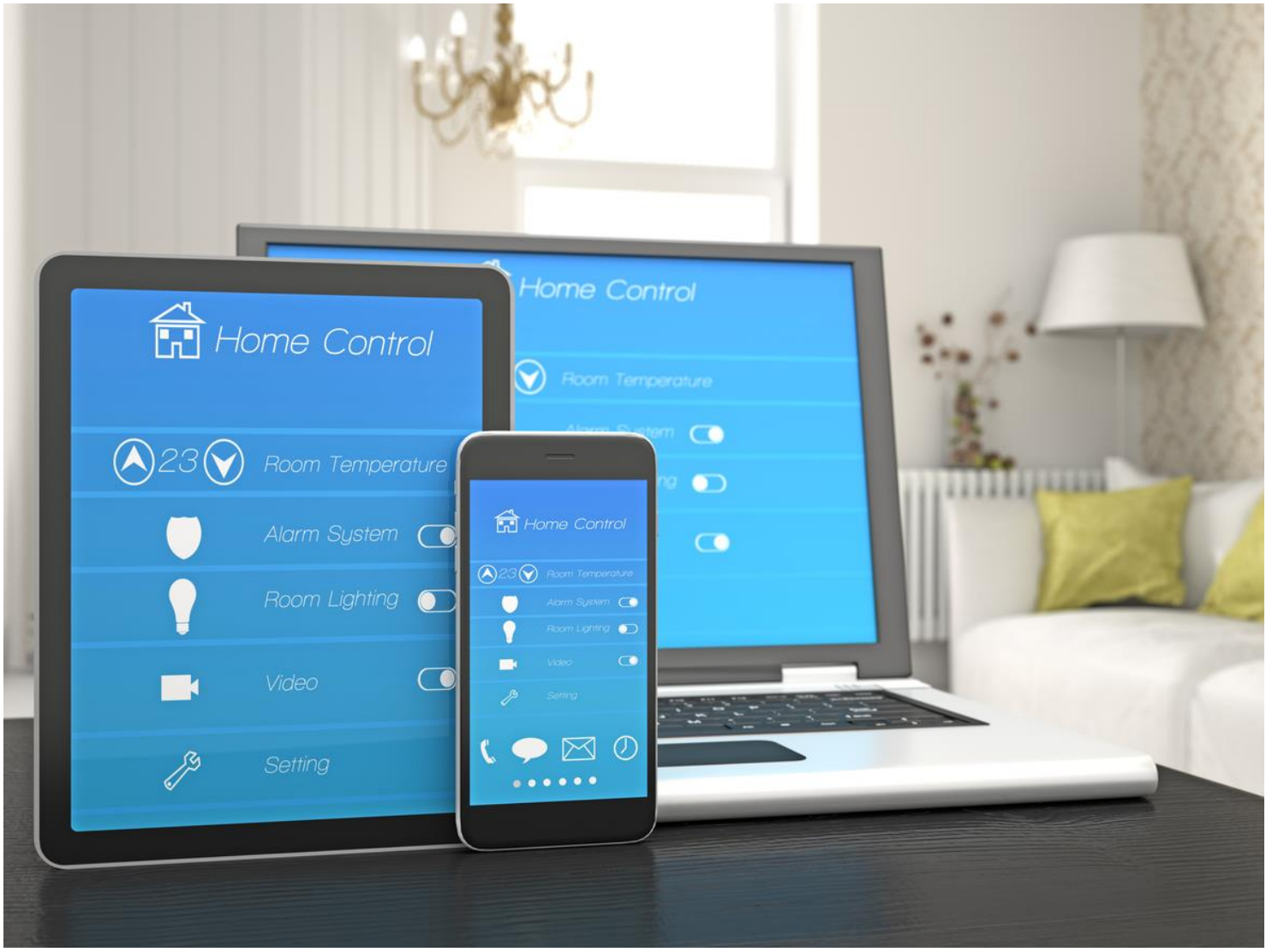
No. 6: Implement an agile approach.

While digital transformation is a multiyear journey, perhaps counterintuitively, it should not be over planned. The current rate of technological change and increasing interdependence between industries diminishes the value of highly detailed long-term plans. It is simply too likely that the context will evolve before the strategy is implemented. So, make sure the strategic approach to digital transformation is flexible enough to adapt to change.

The most reasonable way to start the process is to explore the value digitalization can bring to specific markets or products and start where it will solve most problems or bring most benefits. An improved experience is likely to have the most impact in areas of highest customer activity, and in the largest and most cumbersome processes.

No. 5: Tune IT infrastructure to support digital strategy.

The dynamics of change place a high value on operational and strategic adaptability to shifts in competitive landscape, customer needs and market conditions. One of the roles of IT is to enable adaptability as well as rapid digital development (rapid release cycles, automated testing and deployment) and dynamic interactions across the partner ecosystems. IT architectures must be reconfigured, enabling redesign of the front-end systems to deliver smart, customized, intuitive, rich user experiences and their integration with back-end business operations and data.



The dynamics of change place a high value on being nimble when it comes to shifts in competitive landscape, customer needs and market conditions. (Photo: iStock)

No. 4: Instill a culture of customer focus, innovation, collaboration and learning.

Nothing is sustainable without the support of organizational culture. To drive digital excellence, a culture of customer centricity is key. It is also imperative to evolve the type of culture that discourages internal competition and rewards collaboration and mutual learning. For example, the digital team and the IT infrastructure team often have conflicting values and yet their cooperation is essential for successful digital transformation to occur.

Organizational structures may have to be augmented to promote collaboration. Cross-functional digital teams, formed to develop solutions from the customer perspective, are a good way to encourage customer centric innovation.

Also, digital leaders have test-and-learn cultures that accept failure as a natural byproduct of the innovation process. These cultures are highly risk tolerant and promote and reward quick decision-making and adaptive learning.

Related: The direction of insurance in 2017: It's all about convergence

No. 3: Attract and retain talent.

New kind of talent with practical understanding of digital business dynamics has to be brought in. Insurers must develop strong talent attraction and retention strategies to compete effectively with the leading technology firms and startups for best digital experts.

Look to high-tech startups when it comes to recruiting digital transformation experts. (Photo: iStock)

No. 2: Capitalize on data for personalization, improvement and innovation.

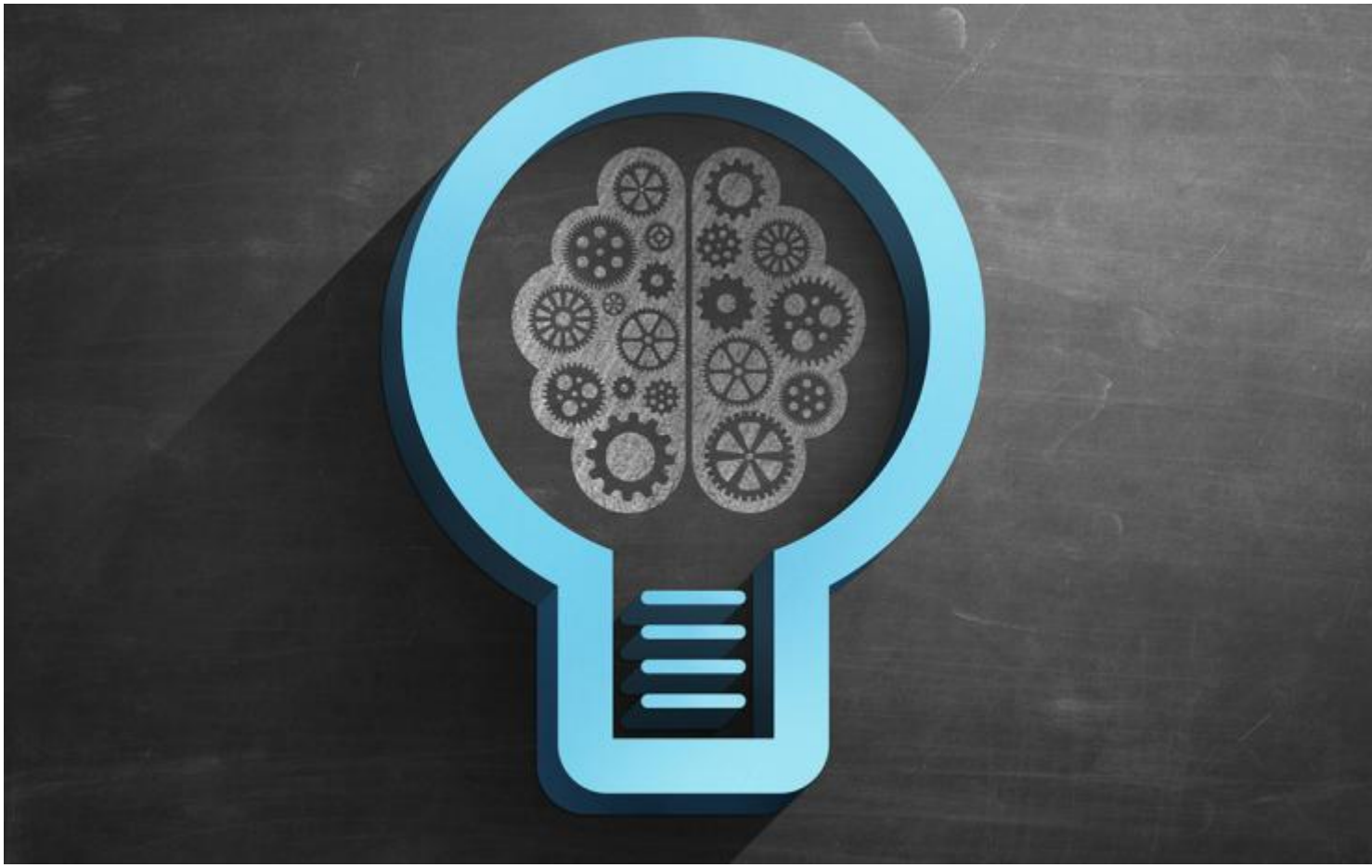
Getting insights from data has always been the key competence of insurers. In fact, their businesses always depended directly on this specific capability. Yet, the new sources and types of data that digital customer interactions will provide (device data, real-time data, unstructured data, big data and so on) are different from structured, statistical data that insurers are used to processing. Getting actionable insights from these new types of data requires new skills as well as data management and analytic capabilities.

Furthermore, a new competence for a digital insurer is to expand its use of data from solely underwriting purposes to using the data to personalize all aspects of client interactions throughout the entire value chain, including marketing and sales, claims, product as well as for operational innovation.

No. 1: Take partners with you.

Digital transformation for an insurer is a group endeavor. Insurance companies are inextricably linked to their suppliers, and it is important to look at the transformation as a process integrated across the supply chain. It is also important to assess who are the reliable candidates for a mutual digital journey.

Academics warn against overuse of machine learning



Backward-looking nature of machine learning could restrict its use in risk management

Lack of data makes AI technology unsuitable for risk management, say Cont and Rebonato

Market participants are increasingly exploring how machine learning can boost everything from credit underwriting to derivatives margin optimisation, but two prominent academics have warned that the technology's applications for risk management are limited. Speaking during a panel discussion at Risk's Quant Europe 2017 conference in London on March 14, Rama Cont, professor of mathematics and chair of mathematical finance at Imperial College, London.

Five Critical Security Considerations for Working with Third-Party IT Vendors

Third-party vendors can be a huge liability for your company's IT security. To help ensure that the proper safeguards are in place to have a secure and productive relationship with its third-party IT vendors, companies should consider the following five-point checklist: (Source: Shutterstock).

1. Become familiar with standardized methodologies.

Existing standards can help you develop your company's security process. The System Administration, Networking, and Security Institute (SANS) Institute has published a Top 20 Critical Security Controls list and so has the National Institute of Standards and Technology (NIST). They standards range from checking your organization's inventory of software, to securing configurations for hardware, software and laptops. They also cover topics such as controlled use of administrative privileges, email and web browser protections, wireless access control and more. Becoming familiar with the standards will help you in the next step of the process when you audit your organization's safeguards.

2. Have your own safeguards in place.

Before you approach third-party vendors, make sure that your own safeguards for company data and systems are in place and you know your company's IT safety procedures and protocols. Some safety protocols that will most likely affect how third-party vendors perform their job include your encryption, authentication and patch management and endpoint security policies. Sometimes there are no quick fixes for weak points in IT infrastructure but that means organizations need to monitor IT weak points at higher levels. This means that management needs to clearly understand where their data sets are located and which vendors will be able to access those data points and systems.

3. Constantly monitor and be in control of third-party vendors.

With IT protocols, processes and tools in place to monitor employees and outside contractors alike, organizations can keep a close eye on third-party vendors. It is important to understand your own infrastructure and weak points before you bring in a third-party. Using monitoring software allows organizations to restrict access to systems only needed for the third-party to do their job. Additionally, depending on the capabilities of the software you choose, organizations can also have the option of defining when vendors can log into systems and from what locations.

Monitoring vendors can also allow you to have the option to only give them access upon manual approval or limit their access within certain applications. In addition, monitoring vendors and keeping records of their access helps mitigate issues by providing the IT with the forensic tools necessary to understand exactly what happened.

4. Do not be afraid to ask hard questions about vendors' IT safety protocols and reporting after incidents occur.

To determine a vendor's security experience, a good question to start with is whether or not vendors have experienced any types of IT security incidents. If the answer is yes, it is not necessarily a reason to not take the vendor. The most important factor to pay attention to is to how they dealt with the incident and how quickly they were able to mitigate or eliminate the risk involved. Another important factor is whether or not the vendors uses subcontractors that have not been vetted by your organization. You should also understand how they assess authorized and unauthorized devices, what their standards are for a secure network infrastructure and what their training is like for security incidents. In addition, ask for a list of tools they use and have your IT team review and approve them. When vetting vendors, try to understand what they believe a viable service-level agreement for your organization can be, what their response and availability time is expected to be, how often you can audit them, and make sure they fully understand your expectations for reporting and incident disclosures.

5. Delegate responsibility to have someone manage the third-party and constantly check-in.

Choose someone that deeply understands your company's networks, infrastructure and general IT landscape to manage the third-party relationship. It is important they know the roles of the vendors, what they should be able to access, and are part of the process when you vet the vendor and ask the hard questions. They need to understand that they are responsible for auditing third parties, and identifying what data leaves the organization and what applications and software come into the organization

More articles by Isaac Kohen »

About the Author

Isaac Kohen is the founder and CEO of Teramind, an employee monitoring and insider threat prevention platform

that detects, records and prevents malicious user behavior.

How to Create a Cyber-Savvy Corporate Culture

When it comes to cybersecurity, the conversation normally focuses on technology, policies and processes. But too often these discussions overlook a critical component: people. (Source: Shutterstock).

According to research from the Ponemon Institute, employee mistakes account for one-quarter of data breaches. While deploying the latest in cybersecurity solutions is critical, an organization's data protection depends upon the "cyber IQ" of its entire workforce, from the mail room to the board room, making it vitally important to cultivate a culture of "cyber-savvy" employees. The following three steps can help organizations reach this goal, regardless of their industry segment:

Embed Cybersecurity within the Corporate Strategy
All corporations, whether they sell sneakers, appliances, greeting cards or cheeseburgers, should recognize cybersecurity as a core business component. Fortunately, many companies are starting to understand this: One-third of finance and line-of-business executives now view cybersecurity primarily as a business enabler, according to Cisco's Cybersecurity as a Growth Advantage white paper. Additionally, 44% feel that cybersecurity practices provide a competitive advantage. More than 70% believe data risks hinder innovation, and 39% have halted mission-critical initiatives due to these concerns.

This new wave of thinking must take hold organization-wide, and change must begin at the top. If the CEO and fellow C-level executives do not include information assurance within every phase of strategic planning, then how can they expect employees to do the same in performing their day-to-day tasks? In leading by example, senior management can clearly demonstrate that cybersecurity *is* business and needs to be built into every process from the very beginning.

Educate Employees about their Role in Security
According to the Ponemon Institute research, training efforts reduce the cost of every compromised record by $9. But organizations will gain far more benefits by avoiding a "one size fits all" approach. Training sessions should address employees' specific roles and responsibilities. A finance professional, for instance, deals with data that is essential for audits or budget planning. A marketing team works with customer-focused analytics. So there really is no training "template" to teach both groups how to do their jobs effectively while ensuring the safety of the data.

In addition, companies need to view training as a commitment to ongoing, continuous improvement. "One off" sessions will deliver little lasting value. At Cisco, for example, every employee is tested about phishing exploits once a quarter. Why? Because phishing represents the most common source of endpoint compromises. With the

stakes so high, we show employees what a phishing scam looks like, how an adversary will “disguise” a malicious link to appear legitimate, and we test what they’ve learned using phishing email scenarios. We created “Phish Pond,” an internal portal where employees can learn how to spot and avoid these deceptive “hooks.” We also make use of online polls and quizzes to reinforce best practices.

A continuous improvement philosophy supports a cyber-savvy enterprise in multiple ways. By routinely revisiting these topics, we are able to update key information as needed so our team gets the most relevant, timely intelligence. Threat tactics are always changing and increasing in sophistication every day so our training programs must adjust accordingly. What’s more, through repeated sessions, we observe that our employees quickly master the “basics” about cybersecurity, which allows us to take them to the next level of training to elevate the breadth and depth of their awareness.

Make it Personal

Thanks to mobile technologies and Bring Your Own Device (BYOD), private and professional lives are blurring more than ever. Work-life balance means something different today than it did just five years ago. Everything is interconnected, with employees accessing personal and work-related emails on the same device. Their use of social media is similarly intertwined – when is Facebook, LinkedIn, etc. a business outlet and when is it a “my time” thing? Oftentimes, it is one and the same.

Instead of ignoring cultural phenomenon or, worse, pretending it does not exist, should help their people safely tend to their personal matters, such as online banking and personal shopping, while they successfully pursue strategic goals for the business. This results in a win-win situation: Leadership obtains further assurance that private activity will not jeopardize business, while staffers feel engaged and confident that their company “has their back” in protecting what matters to them.

By combining these three steps, cybersecurity awareness is no longer perceived as a “checkbox item” or a bothersome distraction from our daily responsibilities. It is embedded into the company strategy from start to finish. Employees soak up new and compelling insights about attack methods in presentations that directly speak to their individual roles. Then, the heightened vigilance extends to their personal lives, expanding the concept of data defense as something to think about every time one connects to a device, whether for business or pleasure. Cybersecurity is a fully realized part of the corporate culture, as much a part of the water cooler discussions as last night’s football game or *Dancing with the Stars*. And this degree of cyber-savviness within a workforce will prove every bit as formidable to hackers as the latest and greatest security tools.

About the Author

Steve Martino is vice president and chief information security officer at the Cisco Security and Trust Office.

Best Practices to Prevent Data Breaches

Over the past decade, data security attacks have become increasingly prevalent due in part to risks around personal information being accessed from dispersed sources including social media networks, email, mobile applications, personal banking and online marketing. There is a growing awakening that critical data is at risk. (Source: Shutterstock).

Because of the potential for monetary loss or damage to the credibility of an enterprise due to breakdown of its system or infrastructure, businesses have come to realize the importance of investing time and money on risk assessment to not only safeguard the company brand but mitigate monstrous financial losses caused through disaster or incident recovery. The following are some critical data security risk recommendations and best practices that can help companies and individuals protect their assets and operations:

- Reassess your email management. Use multiple email accounts to distribute your personal information to avoid being data theft from one source.
- Generate a robust, complex password. Although data breaches are out of your control, it is imperative to create a password that can endure attacks. Ideally, passwords should be at least 10 characters, and contain a combination of numbers, symbols, and uppercase and lowercase letters.
- Conceal your web browsing clickstream history. To protect against the efforts of marketing companies tracking your online behavior, configure your browser settings so that it blocks their efforts and delete your website history data on a routine basis.
- Back up data on a regular basis. The quickest way to backup files is to plug an external hard drive into your computer and copy the files to it. If you are connected to a network, you can also back up to a network drive on another computer. Make sure important data is always backed up first. Cloud services are a much more cost-effective solution for backups, and data can be restored promptly. As a caution, cloud services are potentially accessible by hackers so if you must entrust data to it, make sure it is encrypted.
- One routine mistake produced in database design is to display detailed, error messages whenever a process is not working. With this, a hacker can determine if a database is a potential victim for an injection attack by analyzing the error message in further detail. To avoid this, implement comprehensive testing scenarios to ensure database applications can immediately fall back into safe mode if a process behaves corrupt and deter any critical risk error messages being displayed.
- Engage an expert to collect and analyze quantitative and qualitative data security metrics across the workplace. These collected metrics should enrich the security procedures in place and provide value to the enterprise. Regular risk assessment is an excellent technique to measure and define security metrics to gain further insights and assess security status and position.
- A database index is a data structure used to improve a query's execution time. By quantifying how long it takes for a particular database index to query a dataset, a hacker can leverage the structure of a database. To avoid this, do not deploy these indexes on datasets that are considered proprietary and confidential.

- Implementing user permissions is a key security requirement. Often, in a scramble to launch a database application, users are often assigned privileges that they should not have. These are the types of risks that hackers likely prey upon to gain masked access to a database. Permissions should only be distributed to essential personnel.
- Implement role-based permissions and capabilities. The information that resides in a database will be queried and accessed by many users. Appropriate levels of permissions need to be established at both the file and the sharing level. At the file level, read, write, and execute permissions, need be to be determined for various user roles with discretion. A temporary employee, or contract employee should not inherit these permissions.
- Data collaboration within the company and with third parties requires careful scrutiny. Views provide simple, granular security and restrict data that a user is authorized to examine. For example, with a customer table, a company may want to grant a salesperson access to a customer details including name and address data but withhold the credit card number. A view can be created that only include the data a salesperson requires.
- Continuously scan your network and email attachments for malware to avoid potential security threats.
- Boost security by implementing two-factor authentication that requires not only a password and username but also a piece of information only the user should be acquainted with, such as a personal identification number, password or a pattern.
- Biometrics can provide a supplementary layer of security. This technology verifies the identity of an individual by analyzing their unique physiological or behavioral features, such as fingerprints. Identification using biometric characteristics is preferred over traditional passwords and PIN-based methods because it requires an actual living person to be physically present at the time of identification. Identification based on biometric fingerprint scanning eliminates the need to remember a password or carry a secondary credential such as a credit card.
- Document recovery plans so that if there is a security attack, there are defined procedures in place, agreed by network administration, security staff, operations and application team's departments. These procedures should clearly detail what steps to take to minimize damage, including incident recovery, disaster recovery and contingency planning, and all team members listed should have clearly defined responsibilities.
- Segment your network data to avoid data security breach. This includes segmenting where critical data and sensitive data is stored, and using firewalls to restrict traffic and data access to and from those network segments.
- Employees should be periodically trained and educated regarding their roles and responsibilities in protecting data security. This will involve establishing defined practices and regulations that promote data security and training employees to identify and avoid workplace security risks.

About the Author

Sophia Segal is a senior computer systems analyst, requirements and risk management subject matter expert with over 14 years IT consulting experience, specializing in risk management, requirement management principals and assessing business-critical risks. She is a frequent speaker on topics involving critical risk and requirements management.