DXC.technology

Industry Perspective

Securing the edges of the insurance enterprise

Insurance companies must take a new approach to protect the wealth of personal data streaming in from vehicles, smartphones and myriad IoT devices.

In a little over a decade, usage-based insurance (UBI) has transformed from an intriguing new pricing gimmick to a must-have option in the product portfolio. Nearly 300 U.S. insurers are now offering some form of UBI, and the number of U.S. policies based on UBI reached 7.1 million in 2016, growing 32 percent in just a year.[1]

Telematics from connected vehicles is just a part of the wealth of data pouring into the insurance industry from a widening array of sources — smartphones, smart watches, smart homes, internet bots, social networks, security cameras, body cameras, health trackers, satellite photos, drones and much more.

This data could support innovative ways to assess and price risk, but many insurers are finding they need to overhaul their existing IT environment, move applications to the cloud and support a burgeoning number of mobile and internet of things (IoT) devices. This technology shift is creating new challenges for securing data and protecting customer privacy on the edges of enterprises.

"As we embrace mobile solutions and rely on connected applications, we're taking our corporate information assets outside of the traditional enterprise fortress," notes Todd Pedersen, director of insurance security at DXC Technology. "Instead of a well-defined enterprise network and a sophisticated, layered defense, we now need to focus on the users of the data. For every mobile app launched to support UBI, you've created a new network that didn't exist at most enterprises as recently as two years ago, and you have no control of the endpoints."

New threats to the enterprise

In the past, security operations teams needed to worry about safeguarding only a dozen or more entry points, which were handled by firewalls, antimalware, identity management and vulnerability scanning. Today, add to that millions of smartphones, mobile apps and IoT devices used by customers, employees and partners, and large enterprises can easily lose sight of threats at the perimeter.

"Insurers are going to need to extend the visibility they've built into their corporate enterprise network to these new consumer-driven networks," advises Chris Moyer, chief technology officer for security at DXC.

This represents a major security shift for insurance companies. "While car manufacturers have had time to focus on the new security implications that they created with connected cars, insurance companies are now playing catch-up on these emerging security issues," says Pedersen.

Tips for securing your enterprise

- **Understand your risks.** Instead of focusing on all IT systems and endpoints equally, identify your most critical data and examine the security policies that cover that data. Assess current capabilities and gaps, and develop plans to move to a balanced position of risk and innovation.
- **Be ready for the next attack.** Regular security assessments are key to the success of any security program. Continually assess your ability to detect and respond rapidly. Make sure you have a fully tested response plan in place to mitigate cyber risk. When an incident occurs, all stakeholders, employees and partners should know exactly what they need to do.
- **Enlist your employees.** Better awareness of good security policies and understanding social engineering threats will increase employee vigilance about phishing attacks and potential data loss. Remember, internal breach-points account for nearly three-fourths of all security incidents. Information access and identity management are critical to knowing who is accessing your data and why.
- **Attract and nurture the best talent.** Demands for emerging IT skills are constantly growing as enterprises expand their use of cloud infrastructure, mobile apps and the internet of things (IoT). Finding and keeping security talent in these areas is an even bigger challenge, which is why many enterprises have turned to managed security services vendors to add skills and knowledge related to threat intelligence, vulnerability testing, ethical hacking, multifactor identity management, and end-to-end security policy, architecture and orchestration. Identify skills gaps you have today and anticipate how they will change in the future to stay ahead of the cyber criminals.

Influencing behavior

Insurance companies are not only using this data to evaluate risk but also to influence customer behavior. The John Hancock Vitality Program, for example, includes a giveaway for a Fitbit or a deeply discounted Apple Watch to track progress on a customer's health goals. The program offers premium discounts and regular encouragement from the company.[2]

"Extending monitoring to detailed health indicators such as heart rate, sleep patterns, temperature and more will allow insurers to customize offers to individuals," Pedersen explains.

Among the major factors driving these new programs are changes in consumer behaviors as they rely on a widening array of mobile devices and demand always-on services.

"Insurance companies have policyholders, claimants and agents accessing information across multiple devices and multiple locations," says Moyer. "They're demanding the same kind of high-quality user experience they get when they book a flight with an airline or order a product online from the likes of Amazon. They expect accuracy, responsiveness and intuitive engagement."

Insurance companies need to transform many of their processes to fit into this digitally driven relationship with policyholders. Knowing more about your customers and the information they need necessitates a security model that directs users to appropriate data, instead of blocking access and making tasks difficult.

"Our goal is to embed security intentionally into all these new consumer-based applications," Moyer says. "This is an ongoing set of activities that we continue to work on with our insurance clients to provide simple, easy-to-use solutions. It requires a holistic approach to the overall enterprise and solutions based on the organization's risk tolerances."

Addressing the rapidly changing enterprise threat horizon

Hackers have always targeted banks, insurance companies and credit agencies for the financial and personal data they hold. In this "brave new world" of consumer-facing apps and IoT devices, criminals are creating new opportunities to monetize stolen data.

While smartphones and connected vehicles are being used to track miles driven per month, in reality, these two types of devices can track nearly every movement and communication customers make.

"Think about it from a criminal's perspective," Pedersen says. "By knowing the information you've shared in a consumer-facing app, I now know where you live, where you work, what time you drive to work and what time you come home from work. It's way beyond just a person's financial information. It's really a person's life."

Cyber criminals are increasingly sophisticated and collaborative, creating rapidly changing threats and new intrusion strategies. Security operations teams must be constantly looking across the enterprise threat horizon to anticipate new attacks and identify compromises.

Even well-patched and endpoint-protected enterprises are vulnerable. Organizations today need segmented networks, enhanced privileged access management and sophisticated detection capabilities.

Recently, ransomware attacks have increased worldwide. While ransomware has been around for years, criminals are now stealing personal data, holding it for ransom and threatening to expose it to the world — in some cases enlisting the media to increase the pressure to pay. So insurers not only need to secure the enterprise, but they also need a clear policy and strategy for potential negotiations with criminals.

Customer privacy in focus

High-profile data losses are fueling concerns over customer privacy and the rights of individuals. This is driving sweeping changes in security and data management all over the world. The European Union's General Data Protection Regulation (GDPR), which goes into effect in May 2018, ensures customers' rights to control who accesses their data and profiles, how long data can be stored, when it needs to be erased and who is notified in case of a breach.

In the United States, industry experts are following new security regulations that went into effect in New York State on March 1. The new rules call for banks and insurance companies to scrutinize security at third-party vendors that provide them with goods and services. In 2015, the New York State Department of Financial Services found that a third of 40 banks polled did not require outside vendors to notify them of breaches that could compromise data.[3] The revised rule also requires companies to perform risk assessments and to design a security program to address cyber risks.

On the federal level, a bipartisan group led by Sens. Deb Fischer (R-Neb.), Corey Booker (D-N.J.), Corey Gardner (R-Colo.) and Brian Schatz (D-Hawaii) is pushing for legislation that would protect consumers from breaches in IoT devices.[4] Senators have called for an interagency committee to study the issue, so it will be several months before anything specific is known about the new legislation.

DXC's Moyer recommends that insurance companies know the existing regulations, track emerging standards and look for ways to differentiate themselves from the competition in how they protect customer privacy. They should look to these regulations as an opportunity to improve security, data management and digital business practices for handling data.

Not only will this safeguard privacy, he notes, but it will help organizations gain insight and even better business outcomes from the data they're turning into actionable analytics.

"Instead of viewing data protection as just another mandated compliance activity, insurers should view it as a way to gain trust with policyholders, improve the overall management of data and eliminate data duplication," Moyer adds. "In fact, a recent DXC Technology study found that up to 40 percent of an enterprise's data is duplicated or unnecessary."

Similarly, security doesn't have to be an obstacle to new digital initiatives if it's built from the ground up.

"At DXC, we have extensive experience leading enterprises through digital transformations while simultaneously building in security," Moyer says. "We understand that the old concept of protecting the fortress behind the firewall doesn't cover the expanding edge of your enterprise. To be secure, it now takes continuous focus on protecting, detecting and responding to threats."

Learn more at www.dxc.technology/insurance

[1] "Usage-Based Insurance Global Market Grew by 32% in 2016 to 14 Million Policies," PTOLEMUS Consulting Group, http://www.businesswire.com/news/home/20170518005743/en/Usage-Based-Insurance-Global-Market-Grew-32-2016, 2017.

[2] John Hancock Vitality Program, John Hancock Insurance Website, https://www.johnhancockinsurance.com/life/John-Hancock-Vitality-Program.aspx, 2017.

[3] "New York State Cyber Security Regulation to Take Effect March 1," Reuters, http://www.reuters.com/article/us-cyber-new-york/new-york-state-cyber-security-regulation-to-take-effect-march-1-idUSKBN15V2OA, 2017.

[4] "S. 88: DIGIT Act," govtrack.us, https://www.govtrack.us/congress/bills/115/s88, 2017.