Full Steam Ahead or Proceed with Caution?

Business leaders balance the demand for technology advancement with the very real threat of cyber security breaches.

A White Paper from VIP Software

November 2016

Full Steam Ahead or Proceed with Caution?

Business leaders balance the demand for technology advancement with the very real threat of cyber security breaches.

Business leaders in the property and casualty industry are pressured to adopt advanced technologies that enable customer collaboration in order to remain competitive in a soft and commoditized insurance market. While competition flourishes, so does the threat of cyber breaches, seen all too frequently in industries that rely on third-party collaboration and that deal with confidential customer data. How then do carriers balance the need for speed and innovation with tightening security requirements?

Need for Speed and Innovation

Insurance CEOs see the speed of technological change as one of the largest potential business threats to their organizations' growth prospect, as quoted by NTT Innovation Institute, Inc. in a recent study from PWC. Heightening this threat, it's clear that organizations need to react and create a strategy to surpass their competition, one that involves delivering services that meet the demands of consumers in a digital world. Customers want easy access, at their fingertips, with immediate response from their insurance company. Unless an insurance company meets these requirements, customers are apt to opt out and switch to one that does.

When purchasing new technologies from a third party, the objective is to provide an improved experience for the customer or to enhance and streamline back office operations for greater savings and efficiency, all positively impacting the bottom line. It's a critical time when the industry realizes it can't fall behind other, more innovative organizations that have adopted digital delivery to customers. There's a need to offer more convenient ways for customers to view policies, enter claims, check statuses, etc. on their cellphones, tablets and laptops to meet their busy schedules. The transformation from analog to digital platforms, which enable multiple connected systems and devices to interact with one another offers new opportunities to add value and offers more availability for insurers to take on other important parts of their value proposition, such as back office systems and legal or regulatory requirements.

Innovating at rapid speeds comes with a price however, and may not always be the best approach. Moving forward with technologies that are not well-thought out or lack regard for the potential associated risks is just that -- very risky.

Cyber Security

The world we live in is vulnerable to threats and liabilities that go along with any rapid adoption of new technologies, both on a personal and an organizational level. **The new norm is not *if* your systems will be attacked, but *when* -- and will you be prepared when it does happen?** Experts who study the patterns that occur in cyber-attacks through unprotected devices and systems say, "Don't risk it"!

There are times when innovators leave out very critical components to secure systems and networks at the sake of rapidly deploying software that satisfies the demands of the market. This is obviously not the right answer, yet at the same time, slowing progress is not the most optimal approach either. So is there a best practice that ensures security and yet allows for rapid development?

Adopting more sophisticated security tools, developing newer procedures to follow across multiple disciplines and knowing what to do when attacks occur is a good start. Even more important is building a better understanding of where our new digital technology and its interoperability is headed.

Internet of Things (IoT)

The phrase 'Internet of Things', garnering buzz in several industries, also applies to the property and casualty insurance industry. At the surface of this new digital world, connecting devices for convenience that can turn appliances in the home on and off directly from your smart phone, for example, creates a plethora of problems for insurance carriers. Consider this: a policyholder uses a smart phone while at work to access devices at home, for instance to lock or unlock the front door, and a malicious attack is launched that causes a loss or the hack provides details to the home that leads to theft. If the homeowner files a claim with the insurance carrier, confusion can occur. Does the insurer accept the claim or deny it due to insufficient evidence or understanding of what caused the loss? If they deny the claim, does the insured party sue the insurance company? Which laws do the courts use to litigate the claim? The circumstances surrounding these new types of breaches are baffling the courts on how to handle the legal ramifications of our new connected world.

Third-Party Collaboration

Another area of concern for insurers is when automated collaboration with third-party companies is put in place, a process that is inherent and necessary to the claims process. Consider the unsecured ways in which insurers share information and accept invoices from third parties, such as: adjusters, contractors, litigators, ladder assist, engineers, etc. via email, paper, fax, file transfer and so on. Is correspondence being sent from a secured platform or from an unsecured gmail or yahoo account? Who is processing the invoices on the carrier side? And is there vulnerability created during the invoice transmission process? How do insurers protect privacy laws and confidential information of the policyholders through these unregulated and risky processes?

Does "S" Equal Secure?

It's assumed that new digital technologies innately address important security issues; but do they really? Security is offered by technologists that develop software, along with the explanation that the transmission of data with an 'S' is secured: **S**FTP for transferring files; **S**SL as the security layer for web-based transmission; and 'http**s**' instead of 'http'; but is it all really

secured? Developers say yes, yet hackers say no as they breach systems using sophisticated tools to circumvent these secured measures. Firewalls are no longer enough. Hackers need only a web browser, a good set of internet tools and a little knowledge.

Trust the Experts

It's necessary to rely on the security experts to secure your systems. They understand the type of data you own and how it's categorized according to governmental agency standards, e.g. whether it's confidential, restricted, proprietary or open to the public. Data must be secured throughout the transmission process, especially at each end-point which includes an additional layer of data encryption, ensuring a greater degree of difficulty in reading and compromising customer information. Certain forms of data need to be much more secured than descriptive data that doesn't compromise a customer's personal or financial information. For example, "PII" data includes personal forms of identification, including name, address and driver's license information, while "PCI" data relates primarily to credit card and payment data. In-depth measures must be put into place to secure these types of data categories and third-party software needs to be accountable.

We've seen with major corporations that even with precautions and security procedures in place, breaches still occur. Consider what happens when security is breached: hackers compromise the data and steal customers' identities or create a massive 'denial of service attack' to websites or even ransomware. If breaches occur even with precautions in place, how it's then handled is critical. Organizations offering web-based systems must have proper alerts, spend the funds needed to monitor websites and systems, and know what to do in each circumstance. Before purchasing hosted systems or developing new software, these steps need to be reviewed and understood at all levels of an insurance organization. Providers of software need to be trained and ready in case of emergency, especially if a breach to financial data where substantial risk is involved has been detected.

Can Technology be Deployed Rapidly AND Securely?

While speed is encouraged so new technologies can be adopted by necessary departments, it's crucial to have the right software provider in place that knows how to address these critical areas of security throughout the development process. The right set of security methods that provide an extra layer of assurance that everything possible has been done to secure the data and transmission between systems is no longer a 'nice to have', rather it's a 'must have'. As organizations purchase software or agree to sign on to hosted systems presented to them as the fastest way to leap forward and beat the competition, the following is a sampling of the questions that should be asked by the decision makers:

1. Does your organization conduct security audits of the systems on a regular basis by an independent third party?
2. Are the systems tested for vulnerability and penetration?
3. What policies are in place within the development stages to address security and does each stage have a sign off that security has been addressed?
4. Does the system standardize processes so that many of the manual ones are eliminated to eliminate human error, especially in back office operations?
5. Is customer data secured with additional encryption techniques?
6. Are the right procedures in place if a breach does occur and are technical employees trained sufficiently to know what to do to address the problem with immediate response?

Property and casualty insurance carriers must push forward to compete by adopting the newer technologies available both to improve the customer experience and to improve back office operations. It's imperative to satisfy the need for speed, while also cautiously being certain that security is addressed by software providers, especially those that host software.

Standardization through automation is key when it comes to back office operations. Manual processes where the human factor is needed to review functions such as invoice and claims payment processes for property and casualty insurers have been problematic in ensuring secure operations. Various studies have been conducted in how these areas become target grounds for cyber-attacks due to a lack of employee understanding of how these processes can be vulnerable. Within a recent IBM study, IBM Security Services 2014 Cyber Security Intelligence Index showed ***95% of cyberattacks were caused by human error,*** including physical breaches through devices left unlocked or more importantly from employees clicking on an unsafe attachment or URL.

Interconnectivity within our digital world is inevitable, introducing more and more automated tools for collaboration. At the same time and with these same tools, malicious attackers will only become more sophisticated in their ability to launch cyber-attacks against organizations that are not prepared or have built relationships with service providers that are not focused on securing data and systems.

It's important to consider both speed of delivery as well as every possible solution to securing web-access and systems, in order to create the best outcome in the end. So charge ahead with pursuing new technologies, but with eyes wide open, especially when playing in the Internet of Things.

About VIP Software

VIP Software enables property and casualty insurance companies to scale their businesses accurately and profitably by providing innovative software solutions backed by white glove service and a commitment to our customers' success.

Our software is built on enterprise-class infrastructure to deliver performance, security and control suitable for demanding production environments. Designed with the technical control and security measures required to meet a variety of regulatory and industry standards, organizations are enabled to meet many of their own compliance and safety requirements. Through our high-performance, private cloud platform, companies maximize privacy and uptime to support rigorous workloads, with access to 24/7/365 support, which we understand is critical to our customers.

Learn more at vipsoftware.com.