5 Security Questions Every Insurer Should Have an Answer For

(and the Answers They Should Have)

OnBase® by Hyland

In **93 percent**

of breaches, attackers take minutes or less to compromise systems.

2016 Data Breach Investigations Report from Verizon

Four out of five

victims [of a breach] don't realize they've been attacked for a week or longer.

2016 Data Breach Investigations Report from Verizon

68 percent

of funds lost as a result of a cyberattack were declared unrecoverable.

Heimdal Security

$301 million

paid to ransomware attackers in 2016.

Datto Inc. Security Study

Don't be alarmed, but if you accessed this eBook via USB drive, you may have fallen for one of the more common cyberattacks perpetrated today: The USB Drop Attack. *(Don't worry, you didn't!)*

The ruse is simple. Data criminals place USB drives in high traffic areas, waiting for someone to pick one up and plug it into his computer, hoping to identify the original owner or see what he found. Instead, the USB drive installs malware, giving the criminal access to the user's data and, potentially, the user's data network.

The ploy is effective. When Elie Bursztein, a Google researcher, planted a number of USB drives across a college campus, as part of a larger security study, passers-by picked up 97 percent of the drives. Of those passers-by, 45 percent plugged them in and explored the files. In the real world, this could kick off a data breach that might cost an insurance company hundreds of millions of dollars in fines and litigation and, more importantly, make public the private information of its insureds.

Keeping security top-of-mind

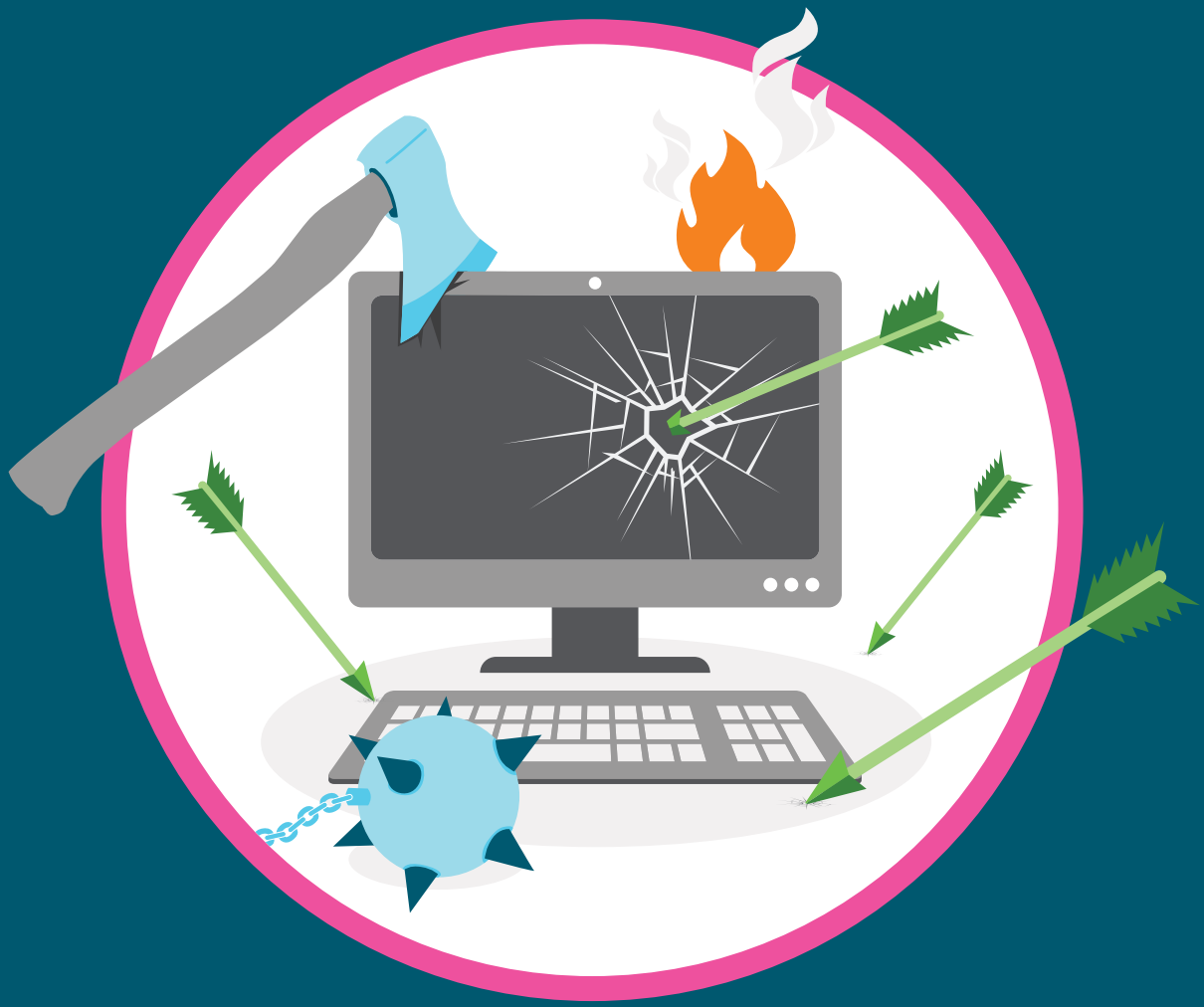
While we strive for digital transformation today and look forward to InsurTech's promise of a revolutionary tomorrow, insurers must not forget that information security is vital in the here and now. Evolving federal and state regulations, like the New York Department of Financial Services' recent cybersecurity law revision, won't allow insurers to forget. The revision requires banks and insurers to meet minimum cybersecurity standards and report breaches to regulators.

Because so much confidential data passes through today's business systems, we expect modern information management solutions to meet a higher degree of scrutiny when it comes to data security. Modern digital systems and procedures must be fully secure to retain the trust of agents and insureds, and to protect companies from liability.

It is time for your insurance company to ask the question, "How exposed are we?" Can you fend off a cyberattack? Are you prepared to comply with the changing regulatory landscape? Are you replacing error-prone, paper-based, manual processes with secure digital versions?

If you're searching for answers, we're here to help.

2015 Global Cybersecurity Status Report from ISACA



Q: CAN YOU FEND OFF A CYBERATTACK?

A: Yes, you can. If you are proactively managing the threat of cyber incursion.

Cyberattacks against insurance companies are becoming increasingly frequent and sophisticated. The threat landscape has changed dramatically over the last decade. Sophisticated and highly automated hacking tools are now widely available, lowering the barrier to entry and contributing to the proliferation of hackers.

There is no security by obscurity

Consider this statistic:

- **In 2016, more than 1.3 billion records were lost in data breaches, according to a study by Gemalto.**

While high-profile hacks of major retailers and service providers, like Equifax, receive the most press attention, many more breaches at smaller and lesser-known companies and organizations contribute to the statistic.

"Security by obscurity" – or believing your organization is too small to be a target – is no longer a viable strategy for information management. Smaller, less protected companies and organizations are prime targets, and these breaches are more likely to go undetected and under reported.

Information theft is a volume business

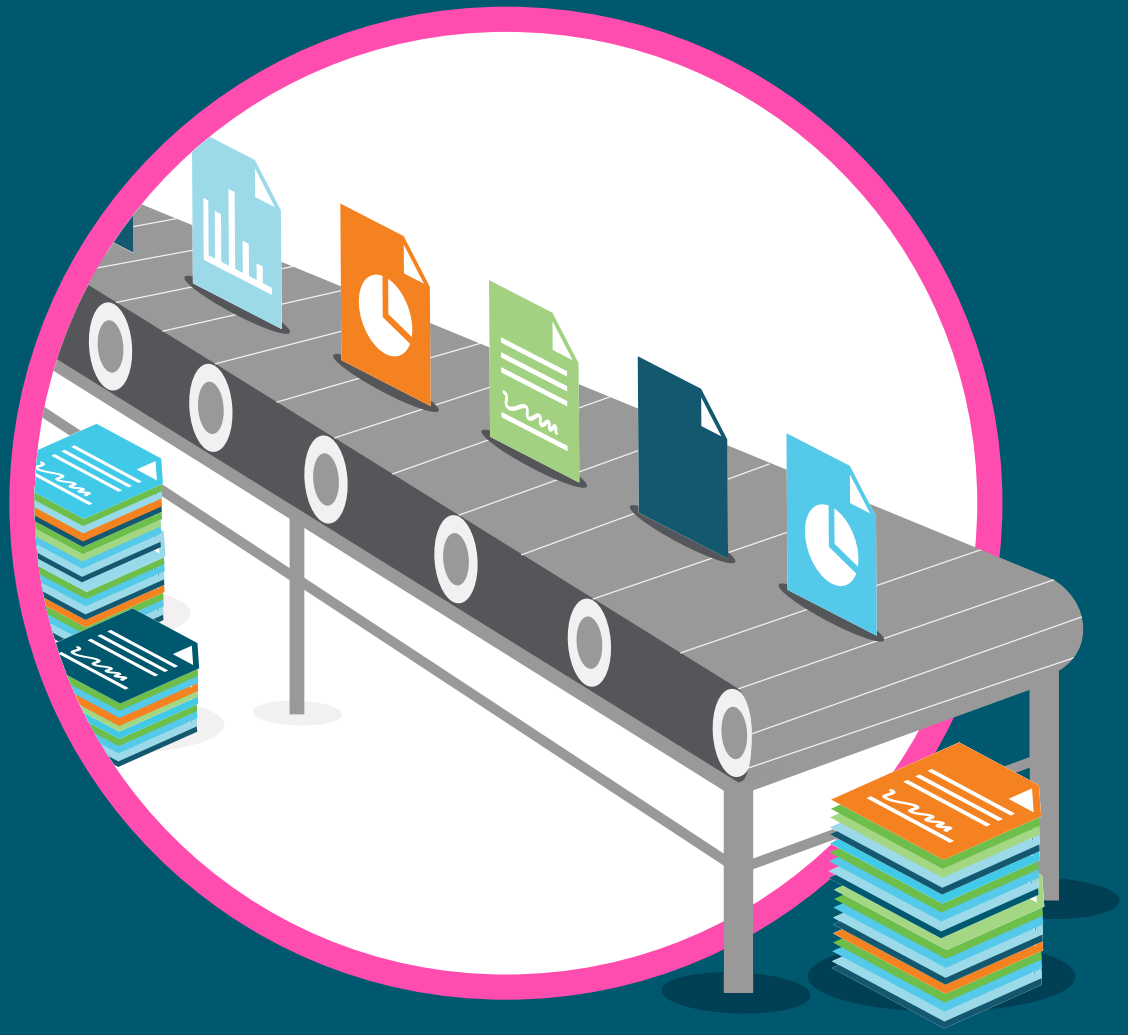
Today information theft is a volume business with a rather mundane objective: Plunder caches of personal information from average people. This personally identifiable information (PII) might include email addresses, website logons, social security numbers, bank and credit card accounts and health insurance data. Insurers possess a treasure trove of exactly that, sensitive personal information from average people, making insurers of every size a prime target.

Furthermore, insurers' integrated information systems provide multiple pathways for attack. Legacy systems with outdated information security protocols create digital weakness and unexpected exposure. Before you know it, a digital pirate has stolen that treasure trove.

Don't treat security as an afterthought. That is the moral of the story. Start at the beginning, prior to evaluating your current legacy system or implementing any new software solution that is going to touch your insureds' personal information. Make sure the vendor considers security at every phase of the solution's product lifecycle, including development, testing and support. You could go so far as to ensure the vendor gives its development and quality assurance employees the tools needed to detect and prevent software vulnerabilities.

43 PERCENT of data breaches [in 2015] were caused internally. Half were accidental, caused by poor security practices, while the other half were intentional, caused by disgruntled employees and malicious insiders.

Intel Security, September 2015



Q: HAVE YOU ELIMINATED MANUAL, PAPER-BASED PROCESSES?

A: Paper is a thing of the past. If not, you may be setting up trusted employees for failure.

Often, when we talk about information security, we focus on technology vulnerabilities. How criminals can remotely access personal information from some unknown and untraceable remote location. While that happens, there is a much bigger threat to the security of your insureds' personal data: the people who work for you. Even with the most advanced intrusion detection and prevention technologies in place, your employees will continue to be one of the largest vulnerabilities in your security infrastructure.

We are not talking theft, either, though that does occur and you should prepare for it. We're talking about common and forgivable human error. If your organization relies on manual, paper-based processes, you unwittingly introduce this risk. Employees can accidently pick up and share the wrong documents, allowing incorrect or private information to make its way to outside parties. Anytime you lack security around personal health or personally identifiable information, you are at risk of a compliance or data breach. You also lack an audit trail, which translates into a lack of control.

Digital transformation comes into play

Here is where digital transformation, in its basic form, comes into play. Insurers need a way to manage the content, cases and processes their core systems can't. This requires filling gaps in core systems such as Guidewire and Duck Creek with comprehensive enterprise content management capabilities, such as capture, document management, secure file sharing, workflow and customer communication management.

Moving away from manual, paper-based processes and toward a solution that integrates with modern core systems and business applications, extends legacy systems and helps accelerate digital transformation, provides a host of benefits, including:

- **Simplifying information access and control:** Provide your employees with a complete view of the information they need, where and when they need it.
- **Breathing new life into legacy systems:** Manage digital documents, electronic forms, web content, multimedia files, emails and more all in the context of your core system.
- **Secure information:** Multiple levels of protection, such as NT or LDAP authentication protocols and easily defined user and group permissions, keep information safe and secure.

72 PERCENT of [3,000 IT professionals surveyed] say they are in favor of the US Cybersecurity Act, but only 46 percent say their organizations would voluntarily participate in cyber threat information sharing, as outlined in the Act.

ISACA's January 2016 Cybersecurity Snapshot

Q: ARE YOU PREPARED TO COMPLY WITH THE CHANGING REGULATORY LANDSCAPE?

A: Yes! If you are keeping up-to-date with each new legislative twist.

"The push for changes in the substance and architecture of insurance regulation, often originating from nontraditional insurance regulatory sources, never has been greater," writes Dave Snyder, VP of international policy, Property Casualty Insurers Associative of America, in Business Insurance. Later, he writes, "We are seeing increased focus on governance, risk management, remuneration and cyber risk."

While the thrust of his column, U.S. insurers face new, complicated regulatory environment, focuses on the economic impact of new legislation, it essentially asks the same question: Are you prepared to comply with this changing regulatory landscape?

Know well the NYDFS's cybersecurity regulation

That includes contending with the New York Department of Financial Services revised cybersecurity regulation, which went into effect March 1, 2017, even if you are not an insurance company doing business in New York. The regulation requires organizations to establish and maintain a "risk-based, holistic, and robust security program" designed to protect consumers' private data.

It is smart to assume other states will eventually pass similar legislation. It might make sense to get a jump on the possibility and adopt some or all of the cyber security best practices laid out in the regulation. That includes hiring or appointing a Chief Information Security Officer (CISO). The CISO oversees and implements your overall cybersecurity program. The best CISOs can explain cybersecurity issues in clear, concise business language and demonstrate the value of the risks managed by the CISO's team.

The new regulation also calls for the implementation of encryption at rest and in transit for all non-public information within five years. Level up and make sure you protect data at every state:

- **Data at rest, or while it isn't in active use:** Make sure your data is encrypted with Advanced Encryption Standard or AES-256 or AES-128, including keyword values and if that data is exported to removable media, like a CD or thumb drive. If any unauthorized users access the database, keywords and other data remain unreadable.
- **Data in transit, or moving between servers and within the database:** AES encryption maintains data security, even if someone intercepts data in transit. Protect communication of data with TLS or Transport Layer Security.
- **Data in use, or data accessed by authorized users:** Ensure your administrator can configure your solution to allow only authorized users access to information. Have configurable session timeouts to prevent unauthorized users from accessing data on a user's screen after a specified amount of time has passed.

California Data Breach Report 2012–2015

Q: ARE YOU EDUCATING YOUR MEMBERS AND EMPLOYEES ABOUT ONLINE SECURITY?

A: They know their personal information is safe and how they can keep it safe. Don't they?

Security, at its most fundamental state, is about access and control. Who has access to information and what can they do with that information? For your insureds, especially Millennials, access and control means even more. They want to make changes to coverage without trouble, easily find answers to insurance questions, and purchase products – all online, whenever they want, and, in many cases, from their mobile device.

Above all else, they want to know their personal information is safe and expect insurers to provide best-in-class online security. This provides you the opportunity to both engage with and educate your insureds about your information management strategy, as well as steps they can take to improve their account security individually, including:

- Choosing long, strong passwords – and different passwords for each account
- Select two-factor authentication, if available
- Know how to secure your social feeds, and make sure to receive account access notifications

Teach your employees, too

Your insureds are only one side of the coin. Your employees stand on the other. Remember when we talked earlier about the effect of human error on security? While much, if not all, of that disappears when you move to a digital enterprise information platform, often employee frustration replaces it. That frustration can produce new vulnerabilities.

How? As organizations become increasingly data-driven, employees need access to more data sources. In turn, expanding regulation and compliance requirements demand increasing controls on how employees access and use that data. Those excessive security policies and procedures hinder employee productivity and increases risk of non-compliance.

Your information management strategy should help solve this security puzzle by intelligently managing access controls and giving users the information they need to get their jobs done without compromising security. A solution built around the concept of secure, role-based access to information can help. Especially when development designs security controls that limit user permissions to the bare minimum needed in order to do their job. Following the "Principle of Least Privilege," this approach minimizes the risk of intentional or unintentional exposure without hindering the user's productivity.

California Data Breach Report 2012–2015

Q: WHERE CAN YOU FOCUS ON OPPORTUNITIES FOR DATA SECURITY IMPROVEMENT?

A: We have some thoughts. Here are our Top 4.

As you decide what digital transformation means to your organization, make sure digital security transformation remains top of mind. Consider the questions and answers provided in this eBook and find out if your answers align. If you are close, that's great. If you're on the same page, even better. Now make sure you:

1 Change data access automatically when roles change

As employees change roles or move to different departments, it should be simple for a system administrator to immediately change their viewing and sharing privileges.

2 Establish a formal review of data privacy and data security policies covering USB and removable media

This falls back to our introduction where we talked about how USB and removable media can act as a Trojan horse for malware.

3 Do not use public storage services like Dropbox, which provide no encryption at rest

Recall how we talked about the importance of protecting your data at every state. It's even part of the NYDFS's new regulation, which calls for the implementation of encryption-at-rest and in transit for all non-public information. If you are using cloud solutions and public storages services that offer no encryption of data at rest, you're putting yourself and your customers at risk.

Sharing via the cloud is convenient, though. So make sure you invest in an enterprise file sync and share solution hosted on a purpose-built cloud solution. One that is in stringent compliance with ISO 27001, SOC and Privacy Shield standards, provides physical and network security with multiple network layers separated by multiple firewalls, specific disaster recovery processes and delivery guarantees and more.

4 Make sure you understand the security frameworks your peers are testing and make a plan to test and adopt one

Your peers face the same challenges you do. Benefit from this by networking with them. Understand how they are addressing cybersecurity risks, educating employees and customers, and ensuring the safety of data at every state. This will help you shortlist possible solutions and suss out issues before you engage with a new vendor.

Mother Nature: A Different Kind of Security Threat

After Superstorm Sandy, reinsurer maintains business continuity – even with three feet of water in the lobby

In late 2012, when Hurricane Sandy, the deadliest and most destructive hurricane of the 2012 Atlantic hurricane season, and the second-costliest hurricane in United States history, struck New York City, it knocked out ROM Reinsurance's IT systems, halted all business functions and left three feet of water in the lobby of the insurance company's New York headquarters.

The company, a long-term customer of Hyland, wasn't sure what to do. It had long since gone digital, but the storm threatened the security of its on-premises solution.

"With three feet of water in the lobby, we were thankful we eliminated paper, but anxious because we weren't sure how to keep our business running," said Marianne Petillo, president and CEO of ROM Reinsurance. "Our data and documents were on our IT systems, and we didn't have access to them."

ROM reached out to Hyland. Together, the two companies devised a plan to move quickly its on-premises solution to the OnBase Cloud. The company regained 85 percent of its business functionality just as the storm was subsiding. It was once again processing claims, sending payments before year's end and completing other year-end closing processes on time.

"Without the assistance of Hyland's cloud solution experts we wouldn't have been able to function, and I truly don't know what we would have done," said Petillo.

2014 US State of Cybercrime Survey from PWC

Pick the right partner to ensure security is not skin deep

As we conclude our eBook and you begin your digital transformation, we have one final bit of advice. Don't go it alone. Find the right partner who will help you establish an information management plan that will reduce or eliminate risk and help you and your insureds realize your full potential.

Remember, responsible software development companies do not treat security as an afterthought. When it comes to secure information management, how software is developed is just as important as the finished product. The right solution should help you reduce risk and improve regulatory compliance, instead of introducing new risks and vulnerabilities.

To commit truly to protecting your data, your partner must implement security principles and tasks at each phase in the product lifecycle, including development, testing and support. Ask your prospective vendor to describe the role of security at each phase in their product lifecycle.

Make sure they follow a strict Security Development Lifecycle methodology to protect your data and systems. This ensures specific security tasks at every stage of product development and testing, and quality assurance. Ask if the vendor trains all development and quality assurance employees on the skills and tools needed to prevent and detect software vulnerabilities.

Only then will you be on the path to a safe and secure future.

One platform
Unlimited potential

OnBase® by Hyland

To learn more, visit **OnBase.com/Insurance »**