CANADIAN UNDERWRITER.ca

Canada's Insurance and Risk Magazine

TABLE OF CONTENTS Apr 2015 - 0 comments

The Little Risk that Could

Brokers' privacy risk is no longer an afterthought. In years past, privacy risk may have garnered far less attention than more commonly acknowledged risks, including errors and omissions. But the little risk has now grown large enough that brokers are well-advised to adopt both prevention and mitigation strategies.

By: Brenda Rose, Vice President and Partner, FCA Insurance Brokers; and Technology Champion, Insurance Brokers Association of Canada
2015-04-01

Once upon a time, not so very long ago, a diminutive risk called privacy dwelled in brokers' offices. He was not a very large risk, at least not compared to his much more substantial siblings, including errors and omissions (E&O), and his chances to expand were limited.

Over time, however, the little risk started to grow, nourished by the increasing information stores to be found in brokerages. Cleverly, too, he disguised himself, calling himself cyber risk, and for a while deflected attention onto technology enterprises. But eventually the day arrived when brokers had to recognize that privacy risk had developed into a full-fledged hazard, a threat requiring concentrated discipline and strategy to tame.

GROWING LARGER

Brokers have always had a privacy exposure regarding their customers' information. Intermediaries must assemble vast quantities of detail, often containing clues as to clients' identity, habits or preferences, which they share as needed with potential providers and, otherwise, protect confidentially. What has changed in recent years, though, is the magnitude of risk.

With the rise of analytics and intensified computing power, the amount of collected information has exploded. Data is much more granular and individualized, and it is recognized as a valuable asset in itself, both within the insurance industry and also by other outside interests. The Internet's rapid-fire delivery has exponentially increased the distance over which information can be dispersed in seconds, while rising litigiousness means that the likely penalties, costs to manage breaches and potential third-party compensation are all climbing apace.

The increased scope of privacy risk is apparent in the numbers from real data breach incidents. Statistics vary widely, but invariably research shows mounting costs. NetDiligence's 2014 Cyber Claims Study, for example, which surveyed insurers on paid cyber claims, estimated a per-record cost of $956, an almost 300% increase from 2013.

The figure represents a full gamut of costs, ranging from corrective technology to notification expenses, production downtime and reputational damage.

All too often, business owners, including brokers, can fail to appreciate the very real dangers created by their own information exposures. This can be a serious mistake. An IBM study shows that financial and insurance organizations, not technology companies, are the most targeted by criminals, while the NetDiligence project noted that 23% of claims occurred at organizations with less than $50 million in revenue.

Breaches do not result only from deliberately targeted attacks; human errors often also play a role.

Brokers must recognize the significance of the personal information amassed within their systems. Protecting that data from exposure using classic risk management approaches, however, can be challenging, when both the threat and the potential damages are constantly changing.

It is also important to remember that standard E&O policies are not intended to respond to claims alleging negligence in protecting privacy.

Even though brokers may acquire custody of someone's information through the course of their business activities, the definition of "professional services" rendered by them would not be deemed to include safekeeping of data. Nor, of course, does standard commercial general liability cover the kinds of loss resulting from privacy breaches. Brokers looking to manage privacy risk through insurance need separate, specific coverage.

Hugh Fardy, senior vice president at the CG&B Group, which stewards a national brokers E&O program underwritten by Swiss Re, confers regularly with brokers learning to manage their cyber risk.

Observes Fardy, "Insurance brokers like other businesses are working to understand and establish their exposures related to the possession of others' personally identifiable information. In conjunction with their E&O insurance, we have made available a minor extension for breach of data exposures subject to confirmation of basic protections being in place. A disappointing number of brokers have elected to take advantage of this offer."

Risk reduction would seem to be a natural approach for insurance professionals such as brokers. Fardy advises that in many cases, a protection questionnaire can serve as a review of the internal protections not yet in place or missing in many broker offices.

GETTING PREPARED The Swiss Re survey suggests five initial areas for brokers to review. These are detailed below:

Train staff regarding the requirements and duties under PIPEDA

Maintaining the confidentiality of customers' information is common sense and has always been essential to the role that brokers play for their clients. Further, brokerage employment agreements commonly re-affirm individual staff will respect the confidentiality of the information with which they work.

Nevertheless the principles laid down in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) legislation, and other corresponding provincial statutes, can be viewed as an articulation of essential practices for protecting clients' privacy within brokerages.

Broker vigilance must extend, too, to the increasing integration with external insurer or data resource systems; insurers and vendors alike can expect brokers to request confirmation that customers' information will be protected and not shared with any other parties, in line with PIPEDA principles.

Among brokerage staff, familiarity with PIPEDA's common standards builds awareness and sensitivity, as well as creates a formal point of reference for the professional behaviour customers expect. Those expectations are rising ever higher, with escalating media reports of data breaches and mass notifications to affected consumers.

Currently in Canada, only Alberta has formal reporting requirements, but pending federal legislation will impose across Canada notification rules similar to those existing elsewhere. Canadian brokerages will need to establish internal action protocols to initiate in the event of a breach to satisfy requirements and public demands.

Implement encryption and other secure mechanisms in place for both the transport and storage of personal information

Because they are so easily lost or stolen, mobile devices of all sorts - phones, laptops or portable drives - can pose a real danger to brokerages. The trend to "bring your own device," allows employees freedom of choice, but magnifies the security risk as central control decreases. Staff must learn to recognize the risks and the need to exercise extra discipline in handling these devices.

A brokerage mobile device policy can lay out basic expectations, addressing such issues as the types of devices permitted, anti-virus and password requirements, and the use of masking or encryption programs, which scramble data so it can be accessed only by an authorized person. Encryption processes can be automated and invisible once authority is established, and applied to entire drives or individual files.

Transport-Layer-Security (TLS), a means of creating email security through encryption provided it is enabled on both the sending and receiving system, has been adopted by a large number of insurers and brokers, and is recommended by the Centre for Study of Insurance Operations (CSIO) as well as broker associations.

Taking the concept of secure delivery to the next stage, carriers and brokers are now working together to establish a similar electronic means of privately transmitting documents and messages to customers.

Utilize passwords and other physical security measures to control access to personal data

Brokerage information systems frequently encompass multiple passwords. For passwords to be effective, the brokerage culture must mandate strict confidentiality around these keys to private information, and they must be sufficiently complex and changed regularly.

Brokerage systems users must appreciate the danger posed by privacy risk, the serious consequences that would arise from sharing or losing a password and, consequently, exposing customer information.

Establish monitoring processes to oversee, manage and review user access rights and roles at regular intervals

Embedded within any password is authority to access various information or functions. Typically, broker management system (BMS) passwords can be customized at an individual level, to suit the various roles within a brokerage.

Access should be carefully planned to tally with the tasks that each person performs, so that no information is exposed more than necessary. The menu of rights granted should be verified regularly and tested, perhaps as part of a periodic internal audit process. Finally, there must be procedures in place to immediately terminate any and all information access for anyone leaving a brokerage.

Create procedures to ensure security events are identified, recorded, reviewed and responded to promptly

One worrisome factor in data breach research is the fact that only detected incidents contribute to the statistics. Far more serious, perhaps, are the lapses that go unnoticed, and may continue indefinitely.

To improve their odds in detecting breaches early, brokers can monitor traffic in their networks, through configurations programmed on their own servers or through their service providers.

Network tools can generate reports that identify patterns and point out access attempts, hacking incidents or other events meriting investigation. These reports generate, in themselves, a massive amount of information, surveying the activity over a firm's entire network and/or website, but are invaluable in establishing baselines for normal activity as well as mapping attacks.

Where specialized expertise is needed, outsourced personnel or consultants are options. For other businesses, the best solution is lodging all information with an outside hosting service that performs tasks such as TLS implementation and network monitoring.

Whatever specific defences are chosen, the investment that brokers need to make to combat privacy risk is, indeed, significant. Beyond budget line items, and even when network operations themselves are outsourced, brokerage leaders must dedicate time and effort to understand and plan the essentials of their information systems and ensure that all staff appreciate and comply with security rules.

The industry's leveraging of data has only just begun; new technologies like telematics, geo-location and the imminent Internet of Things will ramp up potential, but also the responsibility placed on those through whose hands data passes. The test for developments and their controls will always revert to the core objective of shielding customers' information from threats. Brokers must nurture a culture of alertness within their offices and systematically plan the practices that all staff follow.

Privacy risk can never be vanquished entirely. He will continue to lurk in brokerages, seizing on any vulnerabilities. Brokers can keep the risk chained and hungry, though, by using the available tools and maintaining consistent vigilance in their stewardship of the confidential data entrusted to them.

Photos

Larger photo & full caption

File size: 38.2 KB (512px X 768px)

Caption: Brenda Rose, Vice President and Partner, FCA Insurance ...

Related Topics

Brokers
Legal

Monitor These Topics

- **Brokers**
- **Legal**

Disclaimer

Note: By submitting your comments you acknowledge that Canadian Underwriter has the right to reproduce, broadcast and publicize those comments or any part thereof in any manner whatsoever. Please note that due to the volume of e-mails we receive, not all comments will be published and those that are published will not be edited. However, all will be carefully read, considered and appreciated.