A Matter of Control

Brenda Rose
Vice President/Partner, FCA Insurance Brokers, and Technology Champion, Insurance Brokers Association of Canada

The architecture of the security most commonly underlying today's insurer-broker interface, which focuses on insurer-approved and issued passwords, removes direct control over access from brokerages to their employees. A need exists to rethink the approach to return control to brokerages, which have the legal relationship with, and accountability to, the carrier.

"Because that's the way we've always done it," has never been a satisfactory explanation. It does not persuade the 12-year-old questioning his or her parents' requirements, and it fails to convince a few years later, when that now teen challenges the reasons for a teacher's apparently arcane routines.

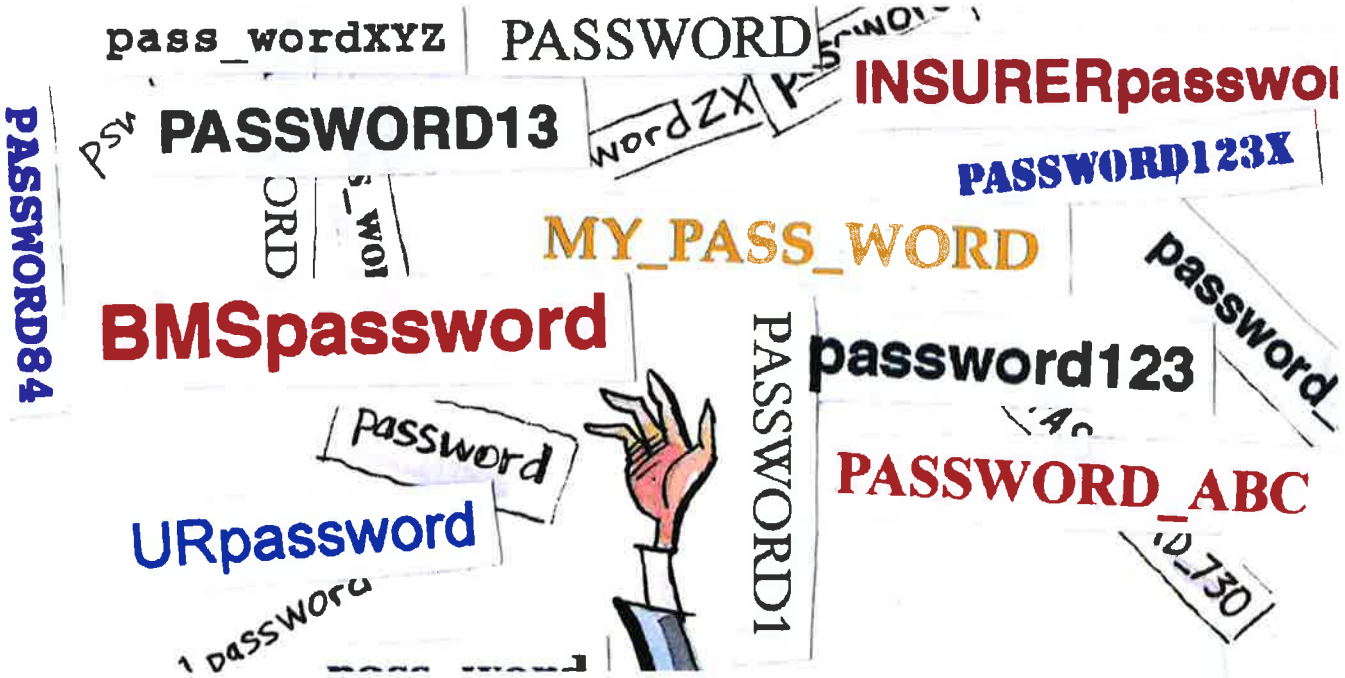
It certainly is not an acceptable justification now for business processes that are ineffective, misleading or even potentially dangerous. Sometimes, assumptions need to be challenged, and often, with new options and information, it is possible to improve on choices made in the past.

OUT OF FOCUS

Brokerages not the focus of insurer-approved passwords

A prime example of one common industry practice that has been perpetuated over time — to the disadvantage of everyone involved — is the typical password-controlled web access by brokers to insurer sites or systems. Of course, the simple concept of redundant data entry into separate broker and insurer systems is a stark inefficiency that many in the industry are working hard to correct. However, the associated security model that has also evolved simultaneously has its own serious, inherent flaws.

Within the framework of broker-insurer contracts, brokerages — rather than individual employees — hold the legal relationships with



carriers. Insurers grant binding authority on a brokerage-by-brokerage basis; indeed, broker-insurer contracts are abundantly clear that brokerages are responsible for errors or omissions, or infringement of binding authority, by their staff.

Broker principals, then, govern their own operations and are ultimately accountable for individual employees' actions. In the course of their duties, brokerage staff members have traditionally communicated with insurers using various tools, including written memos, telephones or, more recently, e-mail and electronic data interchange. Insurers have never determined a particular employee's authority to correspond with underwriters or relay client instructions; that duty has always rested squarely on the brokerage principals' shoulders.

When communication happens to occur electronically, the essential nature of these relationships does not change. The business purposes behind exchanges, and the roles of the correspondents, remain unaltered, and the distinct roles and separate responsibilities of broker and underwriter still persist.

The architecture of the security most commonly underlying today's insurer-broker interface, however, does not reflect this reality. Most often, access requires insurer-approved and -issued individual passwords for broker employees. The focus for granting permission has been shifted away from the brokerage to individual staffers, even though those employees have no direct legal relationship with, or accountability to, the carrier. The brokerage no longer has direct control over access given to its own employees.

When communication happens to occur electronically, the essential nature of these relationships does not change. The business purposes behind exchanges, and the roles of the correspondents, remain unaltered, and the distinct roles and separate responsibilities of broker and underwriter still persist.

Password proliferation may increase security risk

Moreover, with today's typical separate authentication, an average brokerage customer service representative (CSR) working with a number of different insurers will accumulate an overwhelming collection of passwords. Then, in addition to clouding legal answerabilities, these passwords frequently provide admission directly from the Internet, adding great potential for security risk or even abuse.

Dangerous exposures are created when individuals can access insurer systems directly without routing through an identified brokerage's system. If the only prerequisite is an Internet connection, persons who recall their usernames and passwords — or dishonest individuals who steal others' information — can infiltrate insurer systems from virtually anywhere.

When an employee leaves a brokerage, principals must react immediately to cancel each and every insurer password assigned to that person; sometimes, though, principals can be challenged to complete that task if they must rely on backlogged or unavailable insurer administrators.

There are, however, better alternatives available. Integrations between broker and insurer systems are increasingly common, allowing for improvements to some of the old ways of doing business. A recently approved position paper by the Insurance Brokers Association of Canada (IBAC) asserts that the security around broker-insurer transmissions should reflect actual legal relationships and enable control where there is responsibility. IBAC reaffirms brokers' authority over their own operations

and their staff, and advocates an authentication method using a single brokerage-level password, to reflect and reinforce the legal actualities.

Benefits of limiting insurance interfaces to approved brokerage systems

Insurer interfaces that limit incoming broker transmissions to those identifiably originating from approved brokerage systems would eliminate much potential risk, complexity and expense. The insurer would neither be burdened with the task of authenticating individual employees' credentials, nor with the massive chore of maintaining and updating passwords for thousands of individuals.

The use of embedded brokerage-level passwords accessible only to broker-authorized staff reduces the potential for abuse by outside individuals. The insurer system verifies that the incoming message is, indeed, from an approved brokerage and authenticates based on a brokerage-wide password. As such, the information received is sanctioned by that firm. No other incoming traffic is allowed access to the insurer system.

This design works whether a staffer accesses the brokerage's broker management system (BMS) remotely, or if the system itself is hosted "in the cloud." The insurer system can still identify and confirm the origination point.

What will not be acceptable is random access from elsewhere on the Internet — such as a former, disgruntled brokerage employee trying to reach the insurer system from his or her home computer.

The brokerage-level authentication model has recently been tested and demonstrated through a pilot project led by Brovada Technologies and The Guarantee Company of North America. For staff at a test brokerage, client information in The Guarantee's system can now be obtained through its brokerage-sanctioned user IDs, and only via the brokerage network.

Those individuals do not see passwords or user IDs. Further, once a user ID is disabled on the broker network, it is no longer possible to access The Guarantee's system, or for that matter, that of any other insurer employing the same protocol.

Dean Bast, The Guarantee's vice president of national distribution, and vice president and regional general manager for Ontario & Atlantic, says he likes the fact that the design "... allows brokers to control the security within their

If the only prerequisite is an Internet connection, persons who recall their usernames and passwords — or dishonest individuals who steal others' information — can infiltrate insurer systems from virtually anywhere.

(own) system. It removes the onus from the carrier to track individual passwords as the system authenticates the BMS to the carrier seamlessly."

Another way of describing this design is "single sign-on." Although this term has been much-abused, the real intent of this phrase when used in reference to brokers' workflows, is to indicate an individual signs on securely once, into the BMS, and that the authority for any other interface with other systems is dependent on that initial log-on. No other independent passwords or authorizations are required.

Of course, the initiator of any communication, whether brokerage or insurer staff, must still be identifiable for audit purposes. The information identifying an individual user, already built into BMSs, must be part of any transmission.

Brokerage principals must be diligent in ensuring that all user-level passwords are kept secure and confidential, and that access to internal broker systems is terminated immediately should an individual leave their employment.

This is not a new duty, but is much more effectively managed, when terminating a single brokerage password also protects all insurer system accesses.

IBAC continues to remind industry that with evolving technology, automated processes should ultimately follow the logic of the business purposes they serve. A legacy of old assumptions, whether stemming from former software limitations or unrelated outdated procedures, should not be allowed to impair the impact of innovations.

As more and more connections between systems are developed, insurers are asked to consider the following key principles when designing and building electronic interfaces with their broker partners:

- brokerages, not individuals, contract with insurers;
- brokerages take responsibility for the training and actions of their staff, for the authority given to them, and for their access to network and communication resources;
- electronic communications do not alter the traditional broker-insurer business model;
- authentication for conveying information electronically to insurers can be most securely controlled by brokerages when based at a system-level (i.e., brokerage system to insurer system);
- system-based authentication eliminates the additional expense, complexity and inefficiency inherent in individual username-password requirements; and
- individual correspondents must be identifiable, but do not require additional authentication.