Where data security liability ultimately falls for lenders

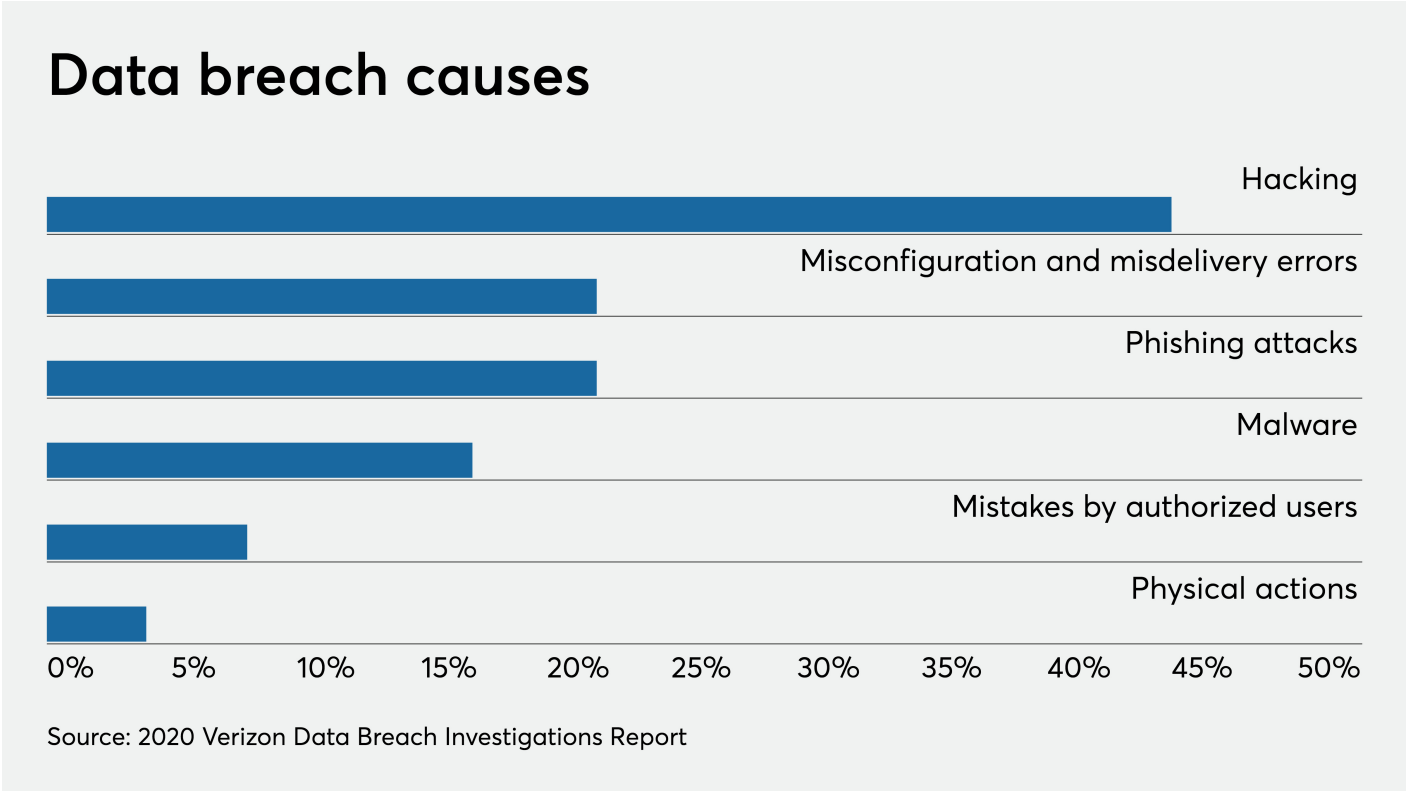
By **Paul Centopani**

May 26, 2020, 2:14 p.m. EDT

The shift to remote work seemingly overnight amid the coronavirus outbreak has meant that employees also swung from directly accessing legacy software to relying on cloud systems like Amazon Web Services, Dropbox and Google Docs.

With the acceleration to cloud computing, how can mortgage companies, who constantly deal with the sensitive personal information of consumers, maintain safety? Where does responsibility fall in the case of a cloud data breach?

In short, both the cloud provider and client share in the security responsibilities. To protect themselves from piracy, clouds go through the secure software development life cycle, enduring vulnerability testing, an installation of firewalls and the use of encryption and tokenized access keys. To protect the physical servers, they're usually located in tornado and hurricane-proof facilities with a restricted few granted entrance.



A lenders' responsibility to protect data overlaps with cloud software provider's duties in three areas: patch management — code changes to update the software; configuration management — maintaining performance consistency; and training employees.

Article **Mortgage brokers and credit unions support their communities during global pandemic**

Typically, the service provider works with the customer to ensure that the guidance and the client's awareness of it are aligned. But no process is infallible. Cyber criminals can penetrate anything connected to the internet and cloud use can create a false sense of security, according to Daniel Eliot, National Cyber Security Alliance's director of education and strategic initiatives.

"We all made a mad dash to start teleworking and some organizations were caught unprepared. They need to make it easy for employees to protect sensitive information," Eliot said.

Culpability questions

With the wide margin of human error, the data owner is often at fault if it's lost or infiltrated, not the data holder. Where liability falls depends on the situation.

Recently both Capital One and Wells Fargo went through widely covered data breaches.

Personal information from 106 million of Capital One's credit card customers and applicants was hacked by a former employee of Amazon Web Services in 2019. She found an entry point through a misconfigured firewall, likely caused by human error. In 2017, Wells Fargo accidentally leaked sensitive data of at least 50,000 of its clients, in what it chalked up as a third-party mistake.

Legal experts say anything within the infrastructure of the virtual machine is the responsibility of the software provider. Operations, verifications and maintaining the software stack by keeping it updated is the responsibility of the customer — the lender in this case. The customer also must do its due diligence on the encryption compatibility of the product and customization of software.

"If the encryption solution the customer deploys to protect the databases is incorrectly configured or they deployed the wrong solution, then they're responsible," said Selim Aissi, senior vice president and chief security officer at Ellie Mae. "If the customer leverages a key management

service or microservice from the cloud provider that's broken and that's the one that gets exploited or has an unpatched vulnerability, then it's the provider's responsibility."

Understanding what caused any breach boils down to the same principles of any other security device. It's a locksmith's job to build and install an adequate lock, but the homeowner needs to make sure it works on their door and turn the key.

Businesses providing cloud services monitor cloud activity, enforce their policies and have the technology and tools to fix any possible weak spots. Hyland Cloud deploys its own compliance group to ensure all the disciplines within the cloud network adhere to its policies. External audits also routinely check that the company meets risk assessment standards.

"When you look at lenders and mortgage servicers, they're dealing with very sensitive information that's not only being handled but also passed to and from a variety of systems," said Bryan Boynar, Hyland's global solution marketing manager. "We apply a defense in depth, which includes numerous penetration testings and multiple firewalls."

But lenders shouldn't be passive about security. They should not store sensitive information in public or free platforms. Systems with multilevel encryption — both for files at rest and in transit — are critical, as is enabling two-factor authentication. If a client notices any suspicious behavior or potential vulnerabilities, it should be flagged to the provider.

"Security is important at all levels, beginning with how the end-user is accessing and traversing the internet," said Marc Cianciolo, global director of cloud sales and operations at Hyland Cloud.

The cloud should only be accessed using a secure wifi network, which is protected by strong passwords or phrases and unique security questions. Hackers and cyber criminals can easily guess at weak passwords and a quick internet search or a scroll through Facebook will reveal your mother's maiden name.

According to Verizon's 2020 Data Breach Investigations Report, hacking was the biggest cause of security violations, covering 45%. The report contains 32,002 incidents and 3,950 confirmed

breaches from Nov. 1, 2018 to Oct. 31, 2019. Phishing attacks and errors — publishing private documents, leaving data storage unwittingly unsecured, or unintentional deletion — followed, each making up 22% of breaches, respectively.

The vast majority of breaches start small, in the form of official-looking emails. They'll contain links asking for credentials or directions to download a file with hidden spyware. In the wake of coronavirus-related layoffs and job losses, cybercriminals have even stooped as low as to start sending phishing text messages posed as links to off-boarding documentation.

Selecting secure software

To find the most secure cloud vendor, lenders and servicers need to weigh multiple factors.

Compatibility of technologies and scalability of the provider's key management need to be considered first. If the cloud cannot scale to the size of the client, it can cause production issues. Misconfigured devices very easily lead to misconfigured services, according to Aissi. Next should come looking at the depth of security control automation and any additional services offered.

Mortgage companies then need to evaluate ease of configuration and monitoring. The customer's ability to use the cloud itself and identify problems before they happen is paramount. After sign up, reconfiguration, operation and maintenance are the customer's job and can become taxing if not initially addressed.

Finally, lenders must gauge a host's disaster support with its recovery time objective — the earmarked time period for restoring business processes following any disruption in order to curtail unacceptable consequences — and recovery point objective — the backlog of files that must be pulled from storage to resume normal operations.

In the case of a breach, there's a thin line between a stroke of misfortune and full-on disaster. Being able to move quickly and compartmentalize damage control can make all the difference.

Of course, cost is the literal and figurative bottom line for businesses. In conjunction with shopping around, mortgage firms should figure out which services they absolutely need.

Tiered storage models broken down by hot, warm and cold types of data retention in the cloud are cost effective, according to Ian Morgan, chief information security officer at Covius. Paying-as-you-go provides flexibility which predictably comes with higher prices for the elasticity.

"You have a very fixed cost in certain situations but in others, it can quickly spiral out of control," said Morgan. "They're not in the business of containing your costs, they want you to use the services. Sometimes what you pay for is a little difficult to understand and you may not know until you get a big bill."

Paul Centopani Reporter, National Mortgage News

Cloud computing **Cyber security** **Data breaches**

Mortgage technology **Digital mortgages** **Coronavirus**