Encryption:

Helping Financial Services Stay in Control of Their Data and Compliance

by Jim Breen

The financial services industry is one hit hardest by the increasing expectations of consumers to access information, receive help and conduct transactions anywhere and at any time via their mobile devices. As a result, for financial services companies, data security is a major challenge. As the amount of client information that they're required to keep secure grows every year, so too does the challenge of doing this effectively.

In the financial services industry's rapid evolving environment, traditional encryption methods have proven too unmanageable for broad deployment by companies. Even when deployed, employees often seek to take shortcuts to maintain productivity, leaving large amounts of sensitive data open to attack.

Cyberattacks cost financial services firms more to contain than in any other industry. The "Cost of Cyber Crime Study" from Accenture and the Ponemon Institute found that the average cost of cybercrime for financial services companies globally has increased by more than 40 per cent, from US$12.97 million per firm in 2014 to US$18.28 million in 2017.

Evolution of Encryption

The long process of encryption began in ancient times when government bodies used it to facilitate secret information during their communication. These days, data travels fast amongst people and places. Encryption is widely applicable for such form of data, that is, when information is transferred via networks, Wireless devices, etc. Hence thinking about security in these areas can help to secure the information, which is usually difficult to physically secure intermittently.

Encryption and Security Within the Cloud

Businesses today expect an on-demand exposure from companies that manage their financial data. The cloud is the key that opens the way for companies to move fast and deliver that experience. More than ever, financial services CIOs face the decision to continue to hold their data in silos or seize opportunities in the cloud for better service, stronger loyalty programs and real-time contextual experiences — across mobile, social and millions of connected devices.

For financial firms, the ability to offer such services gives a competitive advantage, with banks making investments to create and improve a customer-centric digital business model. Aside from benefitting consumers, greater accessibility to data on various devices and applications can also improve employee efficiency.

Personal Data at Greater Risk

Consumer banking is on the rise every day. This shift has led to increasing data traffic volumes as more users rely on applications to interact with their personal data. Addressing this growing volume of traffic has led many financial institutions to adopt cloud and increasingly, multi-cloud environments. The benefit that comes from it is the ease of managing data across multiple locations, devices, without in most cases, worrying about compliance.

While this increases the accessibility of data for consumers, thereby making financial services firms more competitive, it also means that their data spans a larger potential attack surface, making it more susceptible to cyberattacks. As the technologies and data privacy systems become more sophisticated, leveraging artificial intelligence and automation is becoming more important. It is also essential to more effectively detect and exploit vulnerabilities. Financial services firms not only need to engage in digital transformation but to also do so securely – protecting the private data of consumers.

Hence having a technology consultant to help navigate such challenges has become vital, especially for companies that hold financial information of their clients.

Considering Compliance

It should come as no surprise that the financial industry is among the most regulated in the world. There are strong data security requirements for banking and financial companies due to the sensitive and private data that they deal with.

However, in an industry like financial services, it seems that companies are well ahead of the encryption learning curve. But organisations have more than just security to worry about, as the impact of not meeting industry regulatory standards are so high, that companies are now under additional pressure to find a secure and compliant form of communications.

No matter how great the attention to regulatory compliance and to implementing secure technology, there is always one element that it is difficult to control – a company's employees. Clear policies need to specify what employees can do with data. Technology and training should be provided so that every employee understands the reason for the policies and the consequences of noncompliance.

Greater Interest in Encryption

Regulatory bodies these days are taking a close look at financial services firms to ensure they are implementing the security controls necessary to keep their data private. One of the core security features being required by these bodies is encryption. The practice of encryption ensures that data in motion across the network and the web, as well as data at rest in the cloud or data centre, cannot be seen by anyone without the key – even if it is stolen – adding a strong layer of security.

Encryption for financial services firms is being recommended today by several regulatory guidelines, including the new General Data Protection Regulation (GDPR) in Europe.

The Marriage of Security and Productivity

Adopting encryption is an excellent step for financial services firms as it adds a layer of security to your day-to-day operations. Additionally, encryption also provides the ability to comply with a growing number of regulations. However, it is equally important that they can maintain visibility across the security infrastructure without compromising performance, which means being able to see into encrypted data streams.

To achieve this, companies need to evaluate the impact encryption has on security in their business environment and replace isolated solutions with an integrated security solution. Integrated solutions automatically process large amounts of information without slowing or upsetting productivity.

For encryption to work in the financial services industry, firms must make data governance and security an integrated approach within their operations strategy. This includes ensuring critical security and data protection without decreasing the productivity in operations. Encrypted data must be inspected without compromising digital business requirements. The use of automation and high-performance security resources tied together helps extend data protection within the cloud.

Chose your Battles: Security v/s Productivity

When it comes to maintaining productivity, you may be tempted to scale back your cybersecurity policies in order to provide employees more breathing room. It is recommended to fight this temptation. Instead, consult with your organisation's cybersecurity experts and anyone else who has a hand in your company's data and data security. Brainstorm with these individuals to determine your organisation's most glaring or most easily exploitable weaknesses and prioritize them. Your biggest threats need to be secured first.

Client and internal data security should be at the forefront of every strategic technology decision made by financial services companies. At the same time, usability is key to ensuring user engagement. Organisations should consider adopting an IT strategy based on robust security foundations and a flexible architecture.

Adopting a Strategic Approach

Encryption is key to enterprise security, but that alone is not enough. It is only encryption alongside control of a communications system and compliance of employees with communications policies that will protect financial services companies from ever-growing security threats. Ensuring that these aspects are considered in parallel will allow financial services companies to address their data security and compliance challenges and minimise the impact of future cyber-threats.

No single technology or procedure can completely protect the entire organisation. However, with the right combination of solutions, companies can achieve this duality of productivity and security. Technologies that allow for strong privileged access controls combined with solutions to manage the risk of shared credentials and privileged passwords are essential for success.

Jim Breen,

Founder and Executive Chairman of Becloudsmart, a leading global technology company enabling businesses to scale rapidly in a global digital economy.