SecureAge

Data Security for Banking - It's Time to Think Differently

SecureAge Whitepaper 2020

Executive Summary

It is a given that financial institutions are well-versed in security; banks have been around for centuries. They are proficient at protecting transactions and deposits, making security part of their DNA. The modern financial institution continues to apply this DNA to contemporary technologies.

Data security has traditionally been structured around storage repositories. We like to protect information in databases, we use full disk encryption, and we use access controls to manage which individuals are allowed to use what data.

The problem is that when data is moved out of its expected storage location it no longer benefits from the security controls put in place. The data is then completely unprotected – it's a lot like taking cash out of a safe.

Hackers are well resourced and expert at gaining access to and stealing data by removing it from its protected locations. The COVID-19 crisis has increased the vulnerability of data since there are now thousands more employees who are operating outside of the more secure confines of the organisational network. We also can't forget the malicious insider who, in this new environment, no longer has to break through as many security controls.

This paper expands on these issues and then examines an approach whereby security is built right into the data itself. As a result, no matter where data roams, it remains protected and unreadable by bad actors inside and out.

The Reputation and Brand Damage of Data Breaches

Modern regulation has ensured that data breaches are now more public than ever. The fines, damages, and consequential costs may be substantial, but it is the financial institution's reputation and brand that is likely to be hit hardest. According to a Ponemon Institute report [1], following a data breach, financial services organisations can expect an 8% drop in share value, while 65% of their customers will lose trust in the company and 31% will actually move to another provider.

> The Desjardins Group reported costs of $108M resulting from a data breach. A malicious insider with privileged access stole personal information. Part of the recovery package was credit monitoring through Equifax – an institution with its own unfortunate IT security reputation

It is therefore hardly surprising then that the mantra of **Resilience**, **Recovery**, and **Reputation** is embedded in the psyche of IT professionals in financial services. The problem remains – however resilient your systems, if data is taken, then control over it is lost and the stolen information can be exploited. Once word gets out that data has been leaked, reputation and the inevitable brand damage will follow.

Difficulties With Legitimate Access to Sensitive Data

In addition to their large databases of client information and transactions, financial institutions hold a wide range of other data and documents such as trading reports, HR records, meeting notes, business plans, financial statements, reports generated by applications and databases, spreadsheets, and internal memoranda, many of which are highly confidential. Banks in most countries owe a duty of confidentiality to their customers, and intellectual property together with other digital assets also need to be managed and protected.

While individual documents can be and are encrypted and password protected – for example, when price sensitive corporate finance transactions are involved – human error can never be ruled out, especially when several team members are working under time pressures on drafts and redrafts. Encryption for these documents is performed manually, relying on the user both to make the choice to protect each document and to remember to encrypt the data every time. This requirement for case by case decisions creates the risk that files may be stored unprotected, leaving them open to theft.

Due to this complexity it is common for organisations to classify data based on subjective judgements, applying "stronger" protection for information classed as sensitive, and weaker protection for "less important" data. Cost, previous "unsatisfactory" technology experience, and regulators drive this thinking – for example, the Payment Card Industry Data Security Standard recommends that cardholder data is encrypted for both storage and transmission, while other less sensitive information is only protected by access controls.

The (Im)Practicalities of Identifying Sensitive and Vulnerable Data

But to mitigate against all threats as they evolve it is simply not practical to determine what kind of data is valuable and "worth protecting" at any one time, and which information should be less well protected.

For example, an executive's travel plans may not seem especially important, but a hacker could use this information in the form of a social engineering attack to hoodwink the individual or one of their colleagues into approving large transactions, payments, or inadvertently installing malware.

In an ideal world, the IT Security Manager would continually review the data threat landscape, then translate that into updated technology policies which enhance the protection levels for data that is newly designated as sensitive. In the real world, however, this overhead is too great and there is too much other work and "fire-fighting" to be done.

1 Ponemon Institute: The impact of data breaches on reputation and share value

Organisational Evolution Has Delivered a Complex IT Security Patchwork

Large financial institutions tend to have numerous legacy IT systems as a result of mergers and acquisitions stretching back over twenty or thirty years as well as dozens – if not hundreds – of different corporate entities in a wide range of jurisdictions.

As a result, IT professionals need to allocate significant amounts of time to reacting when problems arise in these legacy systems which need immediate attention – for example, security loopholes in a bank's ATM network. A CIO with extensive industry experience that we interviewed for this paper described this process as a "whack-a-mole approach" driven by the practical realities of managing complex infrastructures.

The Data Security Silo

With current IT security we focus on securing data store locations with full disk encryption, database encryption, and application security plus access controls functioning as guards on the doors. The problem is that the data behind the doors is not inherently protected so that someone who gets past the guards can steal the data.

> A report by encrypted storage maker Apricorn indicates that remote workers don't care about data security. More than half of IT decision makers believe remote workers represent a risk of data theft

This siloed approach is taken because it is the pragmatic solution. We know that the data is what is important, but it is easier to protect each data store rather than securing the data itself. We know the problems, but we also know that if trying to force people to take additional steps to increase security – like file encryption or passwords – will at best only reduce productivity but will more likely introduce human error or simply be ignored.

Of course, networks can be monitored for unauthorised data transmission and unusual behaviour, but this is just accepting that the security silo approach leaves vulnerable gaps between data stores.

IT security is hard.

IT Security Education

Using IT security education to keep staff engaged with IT security and being aware of threats is a crucial part of protecting data, systems, and networks.

However, as the sophistication of techniques such a social engineering, spear phishing and deep fakes increases, so does the likelihood of human error. It is just too easy to accidentally click on a link that releases ransomware or other malware.

COVID-19 Adds a New Dimension

And then came the pandemic. Organisations have reacted rapidly and impressively in supporting home working by their employees, especially since conventional disaster recovery plans never envisaged the situation.

This is not just a short-term crisis management issue – the success of home working may act as a tipping point both for employers, who see it as a potential source of cost savings, and for staff, who see it as a way of reducing commuting time and expenses.

> "There will be a long-term adjustment to our location strategy - the notion of putting 7,000 people in the building may be a thing of the past."
>
> Jes Staley, Barclays Bank CEO

This wholesale move to remote working with newly acquired hardware or employees' own devices provides a less monitored and more vulnerable attack vector for the hacker or malicious insider.

In light of this, data security needs to be re-visited to accommodate the "new normal."

Every Organisation Will Be Hacked

"There are three types of organisation – those which have been breached and know it; those which have been breached and don't know it; and those which have yet to be breached." - Chief Information Officer.

> The Capital One data breach, which saw the theft of the personal details of 106 million individuals, was due to insider knowledge gained by a third-party cloud services employee

At some time, there will be an individual with malicious intent operating on your systems, having slipped in between the complex of patchworked security siloes. They could be looking to execute a modern-day bank heist. They may attempt to hold you to ransom or they may simply be gathering seemingly harmless data such as travel plans, personal interests, or staff promotions.

The attack may originate from a hacker, criminal group, or even a nation state. But a compromised user account, malicious insider, or rogue third party services employee who is "legitimately inside" the organisation doesn't need to hack through any security controls – the data is there, in plain text, for the taking. They simply need to move it outside of its secure silo and the theft is complete.

If the data were inherently secure, then it would no longer matter where it was copied – the data would remain secure.

It Is Time to Think Differently

Barriers and access controls that protect the "crown jewels" are important, but it is time to focus on securing the data itself as well.

This requires a switch from a reactive to a proactive data security approach which removes most of the risk elements of human error and malicious intent. By seamlessly encrypting data at source, the impact of data breach is neutralised by ensuring that information becomes unusable the moment it is removed.

SecureAge - Proactive Data Security

SecureAge rethinks security so that data itself is protected rather than simply securing its storage location. The SecureAge philosophy makes security an inherent property of data – in effect tweaking its DNA – in a way that is imperceptible to those who generate and use it every day.

This means that data can be moved or copied to any other location without compromising its security. Even newly generated data such as a database export is inherently secured.

> Personal details of 1.7 million customers of Nedbank of South Africa were made available to criminals through a breach at a third-party service provider who did not employ data encryption

It should always have been this way.

SecureAge protects information in the fundamental data container – the file – using encryption. This takes place in the background so that neither the authorised user nor any application knows that encryption activities are going on. By securing the data within files the information itself is useless to anyone other than an authorised user. Legacy, current and new applications, and databases all benefit from this 100% encryption service without needing any change and without suffering any noticeable performance impact.

Authenticated Encryption

By using per-user or per-service encryption keys, only the authorised individual or process is able to access the data. This "authenticated encryption" builds both data security and authentication right into the data itself. Only authorised users can read data. Even administrators cannot decrypt information which does not contain their own keys.

Privileged users are still able to do their job, moving and restoring files as necessary but they are unable to access file contents. This neutralises one of the most challenging vulnerabilities facing organisations - privileged users and database administrators who are normally in a perfect position to steal data.

Because with SecureAge the data is inherently secured, even a legitimate user who can view information at work will find that any stolen files remain encrypted and unreadable once outside the organisation. This is because authenticated encryption is part of each file rather than an attribute of a data store.

Cloud Data Security

With SecureAge, the Cloud does not represent an increased security risk. Data remains encrypted no matter where it is stored, whether it is in the Cloud, on a server or in a report generated on a home-worker's laptop.

A further benefit of this approach is that inaccurate access controls on data stores become a less urgent concern. And the risk of mis-configuration or of privileged user access by a third party, such as a cloud services provider, is mitigated.

According to a report by cloud security firm Ermetic, "As public cloud is a dynamic, on-demand environment, users and applications often accumulate unnecessary permissions. 80% of businesses are unable to identify excessive access to sensitive data" [2].

Clearly, accurate access controls are important, but with SecureAge the hacker or malicious insider who steals data from an incorrectly secured store will find that the data is encrypted and unreadable.

2 Nearly four in five businesses suffered a cloud data breach in past year and a half: https://www.itproportal.com/news/nearly-four-in-five-businesses-suffered-a-cloud-data-breach-in-past-year-and-a-half/

Process Execution Control

SecureAge provides a further level of protection which blocks the execution of unauthorised processes, including malware, ransomware, and keyloggers. Process execution control ensures that there can be no damage done, leaving servers running, staff working and data available and intact.

This “allow list” facility defends against both external attack and threats from insiders, ensuring that all unwanted software, scripts and fileless attacks are unable to execute.

> Recent high-profile ransomware incidents include Travelex, Diebold Nixdorf and the New York law firm Grubman Shire Meiselas & Sacks, whose files on Lady Gaga have just been leaked by a hacker group.

Hackers are blocked from running malware that steals data, identifies and exploits vulnerabilities, or opens backdoors to the corporate network.

SecureAge - Transparent Data Encryption the Way It Should Always Have Been

The design of SecureAge ensures that users enjoy a seamless experience which makes security natural, inherent, and automatic. The impact of, and opportunity for human error is significantly reduced by completely hiding the processes involved in data encryption, while making sure that only authorised processes may execute – even if someone inadvertently clicks on a malicious link.

By extending encryption to all data no matter where it is stored, the need to use data classification for the purpose of choosing levels of protection is removed. This frees the IT Security Manager from the responsibility and burden of deciding which data is more important than the rest.

The proliferation of cloud services together with COVID-19 forcing widespread data usage from uncontrolled networks and endpoints means that it is time finally to protect the data itself rather than just securing its storage silos. By removing the human element of making security decisions, SecureAge makes file-level data encryption a mainstream reality.

Frequently Asked Questions

Who Is SecureAge?

SecureAge Technology is a data security company headquartered in Singapore with a record of protecting government and enterprise data from the most advanced and persistent cyber threats since 2003. SecureAge's government clients include the Monetary Authority of Singapore, all Singapore Ministries and Statutory Boards, the Singapore Military and the Government of Japan. Commercial clients include NTT, Narita Airport, Sony, British American Tobacco, Temasek Holdings, the Government Savings Bank of Thailand, and GRG Banking.

Why Has No-One Offered This Before?

Early encryption technologies have been disruptive for users and applications, leading to approaches where users were forced to select only those categories of data that were felt to need strong protection. Encryption has been seen as difficult. In light of this, "full disk encryption" has been deployed widely because it implements data encryption without impacting users, applications or servers. This has allowed organisations to check the "data encryption" box. The problem is that full disk encryption only protects a machine that is switched off, and encryption only applies to disk drives where encryption is enabled. Data copied to another drive is no longer secure.

SecureAge's next generation product implements data encryption properly so that information remains encrypted while the system is running and even while data is being modified. It is the data that is important, so with SecureAge, information protection and authentication is an inherent part of the data. By operating at the file system level, SecureAge transparently supports all applications, databases, and services so that no user or app has to change the way they work at all.

What Impact Does SecureAge Have on Performance?

SecureAge employs specialist encryption functions on the CPU so that normal data processing does not have to wait for cryptographic operations. In addition, only the portion of data that needs to be in system memory gets decrypted, leaving the file on disk encrypted at all times. This "streaming" of the data through the SecureAge encryption engine combined with hardware cryptographic functions means that the user perceives no impact on performance.

Which File Types, Formats and Databases Does SecureAge Support?

Because SecureAge works at the file system level, all file types, data stores, and all databases are supported without impact on applications. No software changes are required. Data security and authentication is built into each file so that it can be read and modified without having to decrypt the entire file before use.

Can I Search File Contents Which Have Been Encrypted by SecureAge?

Yes, the contents of all files, such as Microsoft Word, Excel, and PowerPoint or Adobe PDF are still accessible to searches by users who are authorised to access the data.

How Are Obligations Under GDPR and Other Data Privacy Regulations Affected?

Where organisations suffer a personal data breach, the acquisition of an encrypted dataset by an attacker still requires notification to the ICO[3] under Article 33 of the GDPR. However, notification to individuals is not required where the organisation has implemented data encryption that renders the stolen personal data unintelligible to any person who is not authorised to access it.

What Core Banking Systems Will SecureAge Run On?

SecureAge's file system level approach to encryption is applicable across a wide range of core banking systems, including Finastra, Finacle, Flexcube, Temenos and other current and legacy systems.

Can I Implement Higher Levels of Security in Some Areas?

All information encrypted by SecureAge is protected by modern, standard cryptographic algorithms which provide the highest data security. However, the level of security for authentication can be chosen to meet differing security requirements. For example, staff with access to "highly sensitive" information may be required to use smartcards with multi-factor authentication to protect their decryption keys, while other individuals may use "soft" tokens and password authentication for key storage.

Do I Need to Deploy SecureAge in One "Big Bang"?

No. SecureAge can be implemented in a phased fashion at a pace that is convenient for you. Individuals, groups, departments, or divisions can install the product to enhance their data security without impacting the way they work or interact with others in the organisation.

What Should I Do Next?

With information being accessed from uncontrolled environments, the growth in both quantity and sophistication of cyberattacks, and the threat of insider data theft, the status quo must now be questioned.

100% data encryption is already a principle that you accept – full disk encryption fulfils this. But this principle must be implemented better, so that when a file on a running system is copied from one silo to another location, it remains encrypted. Furthermore, authentication should be built into the encrypted file so that only authorised individuals – not the "bad guys" – can decrypt the data.

It is time to take charge of your data with a proactive approach to information security. Get in touch with us to find out more.

3 Article 34(3)(a) states that notification to individuals is not required where an organisation has: "implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption"

SecureAge Technology

Placing real security and usability on equal footing, SecureAge Technology is a data security company headquartered in Singapore. SecureData was first launched in 2003 for the Singapore government, based on a refinement of PKI security techniques. SecureAge made its patented PKI-based encryption an inherent and invisible component of data protection, soon becoming the preferred data encryption partner for additional government and public entities. These long-term and deeply integrated relationships have provided SecureAge with extensive experience of securing the data of large and complex organisations.

SecureAge data security solutions provide public and private entities complete control over data movement within their networks. Every File, Every Place, and Every Time.

Security products from SecureAge have been selected by organisations that need the highest levels of data protection. Customers include various agencies in the Singapore, Hong Kong and Japanese governments; British American Tobacco; Sony; Narita Airport Technologies; the Government Savings Bank in Thailand and GRG Banking.

SecureAge Technology: Our Approach to Data Security

Proactive Protection, Which Is:

Data Security

Data security means pervasive encryption. Data should be secured at the most basic, self-contained unit: the file. Competitive solutions only protect some of the data some of the time, focus on compliance rather than security, or add complexity that introduces risk. Perimeter defences are insufficient as users (the most vulnerable segment of any system) are already inside.

Application Integrity

Application integrity means control through “allow listing” and binding of data to applications. Only authorised processes should access specific data for specific purposes. Traditional anti-malware systems represent passive protection, which is too late. They focus on previously known malware and attempts to stop malicious processes that are already active.

Usability

Usability means inherent and invisible technology. Solutions should remove the human element entirely rather than try to account for or change it. Training and monitoring don’t work all of the time, and if the solution is not natural, people will create their own (non-secure) methods. Users should be able to work just as they want or need to without additional considerations.

No Trade-Offs

In SecureAge there are no trade-offs between these principles, and especially, usability is not sacrificed to strengthen data security. Recognising that individuals will find other ways of achieving something if the “proper” way is difficult is a fundamental principle of SecureAge product design.

Find Out More

Please get in touch to find out more about SecureAge’s enterprise data security solutions. We’re happy to discuss the ways in which SecureAge can improve your data security and arrange a free trial: protect@secureage.com.

Website www.secureage.com
Contact protect@secureage.com

SecureAge

Singapore 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
United Kingdom 74 Mackie Avenue, Brighton, BNI 8RB, Company No. 11734665
Japan 1-16-6, Toranomon, Minato-ku, Tokyo 105-0001, Japan
North America 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA