Information security requires technology that fits people's behaviour & streamlines processes

ABOUT STONEHAGE FLEMING

Advising on over $40bn of assets on behalf of around 250 families from 11 offices in 7 jurisdictions, Stonehage Fleming are one of the world's leading independently owned family offices. They help their clients to manage their wealth and protect their legacy for generations to come.

Chief Information Security Officer, Michael French, has worked in IT and Information Systems for over 20 years, with experience of providing consultancy to numerous financial and legal institutions. Over the years Michael has spent with Stonehage Fleming, he has instigated and established their Information Security team and significantly enhanced the firm's security posture.

THE INFORMATION SECURITY CHALLENGE

Given the nature of Stonehage Fleming's business, it's crucial that client information is kept confidential and thoroughly secured. To be confident that sensitive information is comprehensively protected, Stonehage Fleming wanted to ensure they had full control over who is able to access what, where and when.

KEY RISK AREAS

◊ Access to IT resources; limited to known personnel with privileges aligned to the needs of their roles, including approval of remote access requests.
◊ Physical site access across many locations; restricted to known personnel and the needs of their roles.
◊ Management of identity-based access controls; covering the complete lifecycle of each staff member's employment, with the assurance that all logical (IT) & physical (building) access rights are revoked immediately when personnel leave.
◊ Unattended information access possibilities; preventing computer workstations being left while still logged-in, or documents lingering on printers before collection.

REGULATORY LANDSCAPE

The Financial sector in general is having to accommodate many new regulations, some requiring far more personal information be stored for traceability, and some requiring far more transparency to promote competition. At the same time there's also a new European General Data Protection Regulation (GDPR), affecting all sectors and demanding tighter control over the handling of personal data, with the ability to impose punative penalties for non-compliance.

Because cyber-attacks continue to evolve, and data breaches are as likely to be the result of insider action (unintended or and malicious), GDPR avoids prescribing specific technical solutions to data security, calling instead for the wider organisational requirement of 'security by design'; encompassing people and processes, as well as technology.

"With their understanding of multi-factor authentication, and how logical and physical access controls can be combined, Dot Origin was able to show us the ideal solution".

Michael French
CISO at Stonehage Fleming

TAKING A HOLISTIC APPROACH

Stonehage Fleming could see that these risk areas needed be addressed collectively, rather than tackling each one in isolation, in order to deliver the desired level of security within a real-world working environment. The solution needed to be holistic; fitting-in with how the organisation's people work on a daily basis, and manageable through straightforward, robust, company-wide processes.

For example, while Stonehage Fleming was clear that the best access controls for their IT system would employ strong multi-factor identity authentication, utilizing PKI-based smart cards, it was also apparent that unless users actually remove these ID cards when leaving their workstations, thereby locking their computers, there would be an exposure to possible inappropriate access by others.

By making the staff ID cards an indispensable part of their day-to-day work-life; necessary to open doors to get to the canteen and release documents from printers, staff are naturally compelled to carry their cards with them at all times, thereby enforcing their removal from workstations. By the same token, physical access control also benefits, because staff can't lend an ID card to anyone else without losing access to their computer.

Through deploying a single multi-function physical ID card to each employee, staff get the convenience of having one card which satisfies all their day-to-day access validation requirements, making it easy to adopt seamlessly within workflows. Meanwhile Stonehage Fleming can be assured that any identity credential being used is genuinely being used by the right person, in that location, at that time.

While the technologies incorporated within the ID cards had to meet stringent security requirements, it was equally vital that the tools to manage these identity credentials, and the corresponding logical and physical controls, would facilitate straightforward, robust, operational processes to administer access rights across the organisation.

The Credential Management System (CMS) chosen provides a single platform to handle the technologies used for both the logical and physical access systems, with the scalability to accommodate many users over dispersed locations. For IT access control, both one time password and PKI certificate support was required. The Authentication Server used to validate the credentials integrated easily, through open standards, with internal and cloud-based IT infrastructure across the business.

Regional location of Stonehage Fleming's 11 offices

For physical door access and document print-release, secure contactless (RFID) credentials are also embedded within the ID cards. Stonehage Fleming has full ownership of the encryption keys and software used for reading and writing these credentials, ensuring no one can gain physical entry to sites by copying, cloning or spoofing their cards.

Dot Origin's unique EdgeConnector solution directly integrates door access control into Microsoft® Active Directory (AD), so physical and IT access management can be unified and streamlined. For example, any user's IT and building access permissions can be stopped, with immediate effect, with just one update to their profile in Active Directory.

> ***"Its scalability and direct integration with our IT access controls makes EdgeConnector a brilliant product"***
>
> **Michael French**
> CISO at Stonehage Fleming

Managing door access rights through Active Directory provides global visibility, audit trails and control across all locations, in real-time, unlike conventional site-centric systems. In addition, access to any IT resource can now be further restricted based on an authorised user's location, as determined by their door use. So remote access request can be denied to staff known to be on-site, and sensitive applications or data can be blocked to users outside designated secure areas.

> ***"Dot Origin's expertise and guidance has been vital in successfully implementing a holistic information security solution".***
>
> **Michael French**
> CISO at Stonehage Fleming

SOLUTION SUMMARY

Only by realistically accounting for people and processes can the right technology be selected, to reliably control who has access to what, where and when.

A single identity card for each staff member, required for both logical and physical access, enforces the desired use of identity credentials.

◊ Multi-technology smart cards combining both OTP and PKI credentials for two-factor authenticated IT access, and custom-encoded RFID credentials for door access and document-release from printers.

Security management platforms need to be truly integrated and embedded within the enterprise's IT infrastructure to make administrative processes simpler and more robust.

◊ Unified physical (door) and logical (IT) access control enabled through the addition of EdgeConnector to Microsoft® Active Directory.

◊ Two-factor identity validation for IT access for local and remote users through an integrated Authentication Server and PKI certification.

◊ Combined management of physical and logical credentials through a single Credential Management System (CMS) .

FIND OUT MORE

www.dotorigin.com
For help with your own requirements get in touch:

Phone
Europe & Asia
+44 (0)1428 685 861
Northern and Latin America
Toll Free: +1 888-262-9642
Direct: +1 562-262-9642

E-mail
info@dotorigin.com