White Paper

Biometric Access Control Can Ensure Regulatory Compliance

First Quarter, 2014

Overview

The pace and evolution of modern life moves at such a speed that being part of the zeitgeist is often a fleeting moment for technology vendors, even more so when you consider that the next big thing is likely to have been tried and tested for a number of years beforehand. For the biometric sector, however, it would appear that introducing physical traits as a secure means of access control and user verification is fast becoming the preferred option, especially when it comes to physically protecting data in what seems to the outside world to be a virtual environment.

The topic of data center security is one that has been constantly discussed through much of 2013, with the question of who you are seemingly overshadowed by what you know or - more often than not - what can be accessed. In recent months, former National Security Agency operative Edward Snowden has generated headlines across the world, but while his revelations have made front page news in terms of breaching access control protocols, it is worth remembering that his actions brought data security and protection firmly into the public eye.

Taking that into account, companies have become aware that knowing who is accessing what data is an important part of standard business practices or data protocols, with the security of information increasingly a key factor in protecting both reputation and customer identity. Traditional methods of user authentication such as ID cards, keys, personal identification numbers or even passwords are being found to be less reliable forms of preventing unauthorized access at physical locations, with a growing body of evidence that shows biometrics to be the way forward.

With that in mind, this whitepaper will discuss the options that companies need to consider when assessing the safeguards required to protect sensitive information, with data center security seen as a noted concern.

At the same time, this document will demonstrate the benefits of introducing a secure access control system that complies with governmental and industry regulations. This will be achieved by using the successful implementation and product development of Digitus' biometric technology into the business practices and access control protocols of a leading risk management data company as an agreed case study.

Shortcomings in current data center practices

The growth of data centers as a prime location for information storage has increased in recent years. Companies and organizations no longer need to rely solely on an internal infrastructure to store personal information relating to either their current staff or their customer base, hence the need for these facilities to ensure they offer a degree of data security that meets the compliance requirements of both clients and regulatory authorities. This means that those responsible for protecting said data have a demonstrated duty of care to ensure that access systems and user identification or verification are monitored in such as a way that unauthorized entry is kept to an absolute minimum.

However, with great power comes great responsibility, and an increased awareness of potential data breaches within the industry has focused the minds of decision makers within those companies on a need to make sure that adequate defenses are in place. Over the last few years, media attention has been focused on the ability of cybercriminals to hack into an operating system and liberate data, and while this may always be a concern for any company that stores personal information, physical barriers to unwanted access are just as important.

Data center security is no longer just a question of throwing up an IT firewall and assuming that it will fulfill required security compliance procedures. Information technology has evolved at a breakneck pace in the last five years and data centers have become increasingly vulnerable. Many of the traditional means of identification are, more often than not, reliant on minimizing the capacity for human error, with cards and keys susceptible to loss or unauthorized use.

In fact, a recent survey of 321 IT professionals conducted in December 2013 by Palmer Research showed that security was at the top of the list for 74 percent of respondents, with 88 percent of those interviewed citing it as a the main reason for modernizing their current data center requirements. However, while the results of the survey showed a demonstrated desire by companies to invest in data center protection, there are naturally other elements to be considered if that course of action is to be successful.

In terms of how best to initially address any identified concerns or potential holes, the following questions should be taken into account;

- What are the current safeguards in place?
- How does a company monitor who is accessing their data storage facilities?
- When an unauthorized breach occurs, how does the company respond?
- Is there a demonstrated method of confirming which employees are responsible for access control, and how do they dovetail with industry regulations?
- What are the methods currently in place for access control?

The protection of the data itself is a core factor, but firms should be looking at how the current safeguards match up with ever-changing regulations and, importantly, who has access to the facilities themselves. With data breaches seemingly no longer limited to high-tech companies, this also means that companies have to constantly monitor which

employees have access to data servers, and making sure that adequate protections are in place to maintain the safety of information contained within.

Companies also need to understand the risks and potential liabilities inherent in storing data, a scenario that becomes ever more evident when considering the number of high-profile breaches that occurred during the 2013 financial year. Assessing these risks, however, is only the first step, and what becomes more important in terms of security is how that organization moves to fix any perceived holes in data protection procedures.

Eliminating demonstrated risk in data center security through biometrics

As noted above, physical security at a data center is as, if not more, important than virtual defenses. If the data breach events and unauthorized surveillance events of 2013 have taught companies nothing else, then it has brought the concept of access control to the forefront of solvable concerns. With the majority of organizations seemingly still in thrall to traditional means of verification such as key cards or personal identification tokens, the fact remains that these widely available methods of user authentication were primarily designed to make sure that people were able to enter or exit secure parts of a building without question.

What has become increasingly obvious, however, is that these methods of control are not the most secure way of protecting sensitive and increasingly valuable data. Recent breaches in the retail sector have shined the spotlight on how quickly a company can find its reputation tarnished when data is lost or misappropriated, and while biometric technology is familiar to those who travel extensively, it is making significant inroads into the private sector.

The challenge - as with any emerging or disruptive technology - is to ensure that the implementation or integration of biometrics into a data center strategy fits in with the overall security protection aims of a company or organization. Throughout 2013, biometrics has been frequently cited by security experts and industry analysts as one to watch for the coming years, although the decision by a leading mobile device manufacturer to make it an integral part of a smartphone certainly helped to make it a topic of national conversation.

And while widespread adoption by smartphone users is welcome, it only scratches the surface of what biometrics can bring to data protection protocols and procedures. After all, a biometric characteristic is a measurable factor that is unique to the individual themselves - fingerprint, face, iris, voice, vein pattern or hand geometry - and is typically used not to recognize an identity (such as a password or PIN) but rather to verify a user through the collection of stored biometric data. For example, fingerprints are a distinctive physical signature that are difficult to replicate, especially in terms of providing a live copy that would be able to match the information held on file.

With that in mind, biometric authorization can provide companies with a demonstrated method of access control in a physical data storage location. Users have to be present to enter a secure area such as a data server cabinet or cage, an important element that may

not always be required by those who still rely on the more traditional methods of authorization previously mentioned.

Naturally, there are many factors that have to be taken into account when assessing the impact of biometric technology into a company data security policy. Organizations need to make sure that enabling access is not restricted by a limited user base, with biometric security systems often requiring at least two people to enter at the same time. There is also a requirement for firms to limit what is known as passback or piggybacking - in other words, users accessing a secure area on behalf of somebody else and allowing them to move through a checkpoint without the relevant credentials.

However, it is precisely the ongoing elimination of any perceived loopholes through biometric verification that provides value and, more importantly, the physical security requirements of a modern information technology-based society. This dovetails into the need to protect data, not only as good business practice but also for regulatory compliance and as a demonstrated security commitment to customers or clients.

Case Study - RSA

In 2011, Digitus Biometrics was approached by US-based RSA - the security arm of EMC - to determine the most effective means of protecting sensitive financial data held in four colocation data centers situated in both the United States and Europe.

The firm, a leader in security, compliance and risk management solutions, had recently undergone a Payment Card Industry audit relating to a major player in the financial services arena, one of many such companies that are clients for RSA. Auditors had highlighted areas of concern within its current operating practices with regards to the security of information being stored by RSA as part of its agreement with the well-known financial services company, with data server racks and access monitoring coming in for scrutiny.

While the company was able to confirm that there had been no demonstrated data breach at the time of the PCI audit, it was felt that the use of colocation facilities as a means of storing information for financial services customers meant that the firm was susceptible to unauthorized access to data server racks by non-company personnel within those physical data centers. RSA, a firm with hundreds of clients worldwide, saw the PCI audit as a perfect opportunity to beef up security procedures within the organization, and introducing a two-step authentication system common in biometric security systems was seen as the solution.

According to Vincent Amato, senior security engineer of software-as-a-service operations at RSA, the decision to investigate the potential for biometric procedures was all part of an ongoing drive by the company to make sure the right people had access to data at the right time. Over a period of months, both client and biometric security vendor worked together to identify where any potential breaches could occur and where fingerprint scanners could prevent any such loss of data.

"Anytime you deal with a breach can be very serious and cost the company money," said Amato. "Reputation within the industry can be affected, along with the possibility of losing that particular customer if something was to occur. The more control you have as to who

can access the system, the better off you are. With the Digitus system, we are able to work with the vendor and establish a 2-point authorization system where our system meets these particular security needs and keep it under our control."

One of the benefits of introducing a biometric system with a demonstrated user audit trail, Amato noted, is that it puts user verification firmly in the hands of the data protection company themselves. RSA currently has 80 staff members who are authorized to enter data server cages on both sides of the Atlantic, although the individual nuances of the installed technology often mean that some employees can only access facilities in the United States and vica versa. It is extremely important that there are varied levels of control across the system, especially when taking into account the aforementioned concept of right person at the right time.

In Amato's opinion, this was one of the crucial elements of the partnership with Digitus Biometrics and its biometric access control technology - so much so that it ensured that the company was able to pass required PCI audits in 2012 and 2013 with 100 percent compliance and no recommendations for improvement of the physical security scheme.

"Utilizing fingerprints is most secure over PINs, cards or other items," he said. "What led us to Digitus was the willingness to work with us to 'improve their product' and meet our needs for the various audits."

Conclusion

Biometric security is now arguably one of the technology trends to watch in 2014. With more emphasis than ever before being placed on the value of information, data servers and centers are increasingly in the front line when it comes to being protected from malicious or unauthorized attacks.

At the same time, companies need to be aware of the risks that unsecured user identification can bring, especially for those who still rely on elements such as key cards for access control. Physical security is no guarantee of regulatory compliance, but biometrics is proving to be the most secure way of ensuring that the right people are able to access the right data storage facilities, while providing the company with a demonstrated audit trail over a single networked platform.

Sources

Phone Interview with Vincent Amato, 26th November 2013
Press Release provided by Digitus, dated March 2013
Whitepaper provided by Digitus, dated First Quarter 2011
http://www.esecurityplanet.com/network-security/security-big-part-of-data-center-modernization-plans.html
http://www.nsa.gov/ia/_files/factsheets/i73-009r-007.pdf