SecureAge

Evaluating encryption with the NIST Protect framework

SecureAge Whitepaper 2020

IT Security Today and How We Think About It

A variety of cyber security frameworks exist to help organisations in different sectors to go about IT security in a rigorous and controlled manner. To name a few, there's ISO IEC 27001/ISO 27002, the US NIST Cyber security Framework and the UK NIS Regulations Cyber Assessment Framework. The frameworks are an excellent way to help formalise the process of implementing and maintaining effective cyber security strategies through defined structures containing processes, practices, and technologies which companies can use to secure network and computer systems from security threats.

Attacks still get through: Even with all the time spent and budgets deployed working with cyber security frameworks, however, attacks still get through and data still gets stolen. While it will never be possible to eliminate all data breaches, this paper shows how encryption technology can be used to minimise the loss of information and the resulting impact on the organisation.

> *"Accepting the fact that some [malware] will get through will help you plan for the day when an attack is successful, and minimise the damage caused."*
>
> UK's National Cyber Security Centre

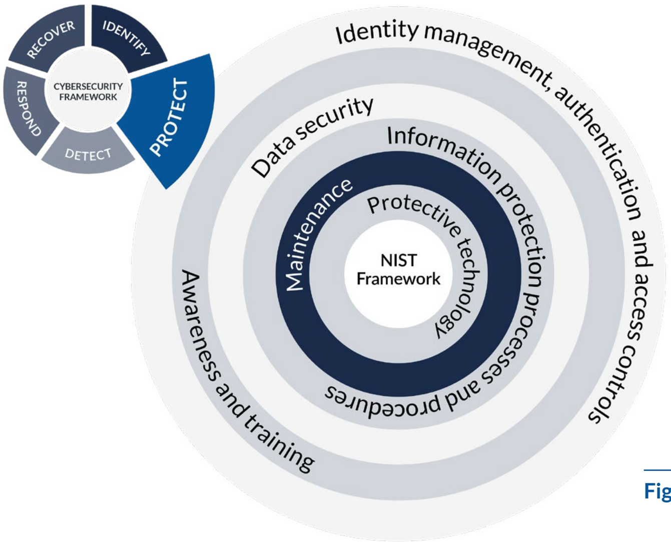

Figure 1 NIST Framework

Document Structure

Cyber security frameworks include a core function: Protecting against cyber-attack. We use the NIST framework to structure the discussion, though the issues raised apply equally to any of the cyber security frameworks.

The following sections list the six NIST categories in the "Protect" framework function, examining commonly deployed technologies within each. For each technology we describe a common data breach scenario, then look at wider security concerns, focusing on data loss or theft. In answer to each security concern, we describe how one product from SecureAge – SecureData – offers a practical solution to the problems highlighted.

SecureAge SecureData protects information at its most fundamental level – through file encryption. Unlike other cyber security products which block unauthorised access to data, or which are selective about which data to protect, SecureData inherently protects all data inside files using encryption.

NIST Category 1

Identity Management and Access Control

Identity Management and Authentication Systems

A variety of user login, single sign-on and multi-factor authentication systems exist that are designed to ensure that only authorised people may access your systems and network. Strong authentication is also important for remote desktop environments which are particularly vulnerable, since the remote machine may already be infected with malware, and anyone attempting access can do so without physically having to hide their actions.

Data Breach Scenario

A legitimate user copies application data to a local file. This file is no longer protected by any controls within the application or database. The file can easily be stolen.

Security Concerns

Insider data theft and compromised user accounts: Users need access to sensitive information so that they can do their job. They are therefore in an ideal position to steal data. This applies not only to the rogue employee but also to a compromised user account.

> A senior auditor at Morrisons leaked payroll data of around 100,000 employees in an attempt to damage the company because of a grudge. The data was exported from a database application then saved to a local file for simple exfiltration

Resolving the Security Concerns

Information must be protected against misuse no matter where it is copied. Even if files are stolen by an insider, or if a user account is compromised, the data must remain secure. Fundamental protection of the data inside the file would protect stolen information.

With SecureAge's SecureData, authorised users continue to work just as normal – but behind the scenes the files they're working with are encrypted. However, if they steal any files they will find that the data remains encrypted. Attempts to open these stolen documents will fail. In remote desktop environments SecureData enforces data encryption, while with SharePoint and other WebDAV based services information is encrypted and secure from the application right through to server or cloud storage.

Access Control Lists (ACLs)

Access control lists (ACLs) and the principles of Least Privilege are designed to provide access only to the information that is required for individuals to do their job. The technique is also applied within databases and applications. Data protection regulations such as GDPR state that only the individuals who have a legitimate reason to process data should be able to do so. Administrators do not have that legitimate need, and should be subject to controls that limit that access.

Data Breach Scenario

A privileged user accesses and steals files containing intellectual property. If an individual has legitimate access to files – access they need to do their job – then they can steal the files. Edward Snowden's actions at the NSA is perhaps the highest profile event of this kind.

Security Concerns

Privileged user access to data: ACLs often allow privileged users to access files which the business would not authorise them to see. This is required so that administrators can move files, restore backups, etc. Secondly, it is the privileged user who sets up the ACLs and can change them in their favour – something that could be exploited by a rogue administrator. Finally, any file, once removed from the organisation, is no longer subject to ACLs and is therefore not protected by them.

> Personal information of nearly 360,000 Quebec teachers was exposed in a data breach. The hackers stole a user code and password, enabling access to the data and facilitating its theft

Resolving the Security Concerns

SecureAge SecureData ensures that each file is encrypted only for individuals who are authorised to access them. This should of course be in line with access controls. If data is stolen, however, files from a SecureData-protected environment will remain encrypted and therefore useless outside the organisation – even if the thief is an insider who would normally have access to the data at work.

NIST Category 2
Awareness and Training

Cyber Security Awareness

Cyber security awareness training is an important component of any organisation's IT security approach. Ensuring that employees, contractors and associated third parties behave in a manner that protects networks, systems and data is a simple but powerful step. However, only 49% of organisations put their new staff through privacy and data protection awareness training and less than a quarter conduct regular refresher exercises[1].

Data Breach Scenario

An attacker carefully monitors a high-level company executive using social media, company press releases and blogs. Armed with this knowledge an email is sent to the target. The email contains specific information that appears genuine, and the executive clicks on a harmful link. Nothing bad appears to happen, but behind the scenes malware is introduced that opens a backdoor for the hacker, enabling data theft.

Security Concerns

People will open harmful items: Busy people or those under pressure will make mistakes. And with the increasing sophistication of spear phishing attacks, social engineering and the stealth of some malware there should be no surprise that some attacks will succeed. Once in place the malware can silently exfiltrate files from your network as well as potentially causing major system and network damage.

> Travelex suffered a ransomware attack knocking their business back to manual processing for several weeks. Commercial clients were unable to offer currency services while consumers were left out of pocket. It is reported that client information was stolen as well, demonstrating disruptionware behaviour

Insiders can install malware: Employees or contractors can be persuaded – possibly for financial gain – to install malware on the organisation's network. This was done at AT&T with the malware in place, undetected for five years.

Resolving the Security Concerns

With SecureAge SecureData in place the malware will be able to exfiltrate data, but since the stolen files will remain encrypted, they will be useless to the malicious actor. It should be noted that another SecureAge product, SecureAPlus, blocks all unauthorised processes from running. This means that the executive in our scenario could have clicked quite safely on the harmful link. The malware would have been downloaded, but when it attempted to execute, SecureAPlus would have blocked it.

[1] Experian/Ponemon Data Breach Study:49% performed training during on-boarding employees. Only 24% performed even annual training

NIST Category 3

Data Security

Data Loss/Leak Protection (DLP)

DLP attempts to ensure that users do not send critical or sensitive information outside the organisation. It achieves this by attempting to recognise and then block sensitive data as it passes through the network. Implementation of DLP is a significant project requiring comprehensive and accurate identification of all network assets and storage locations as well as authorised business processes.

Data Breach Scenario

A rogue employee indicates to the DLP system that their actions are legitimate. Since the DLP has no awareness of business context these activities are passed, and the data is exfiltrated.

> Industrial secrets were stolen from General Electric, the information being smuggled out hidden in the binary code of an image of a sunset. Such steganography evades DLP systems

Security Concerns

Incomplete DLP configuration: There are many variables involved with a successful DLP deployment. Failing to consider all possible avenues of data loss is a frequent path for sensitive information theft, while not spending enough effort on the fine-tuning of the system can lead to inadvertent data leaks. If DLP fails to recognise sensitivedata being exfiltrated then that information is leaked and outside your control.

Resolving the Security Concerns

Since SecureAge SecureData ensures that all data files are encrypted at all times, no accidental or deliberate loophole in the DLP configuration can result in data loss. There is no performance nor operational impact using SecureAge, so encrypting everything just makes sense. Any indication from a user to the DLP authorising their malicious activity and leading to lost data will only result in lost, encrypted data which is useless outside the organisation.

Data Classification and Rights Management

Data classification systems are used, in part, to define the scope of access to, and the security of information, while encryption can be applied to appropriately classified data in order to enforce digital rights. However, encryption is typically used sparingly as it is regarded as being hard to implement, slow in operation and difficult to use.

Data Breach Scenario

A user mis-classifies a sensitive document resulting in a lower level of data protection. Enabling users to classify information can result in incorrect decisions through misunderstanding of the privacy and information security consequences. In addition, automated classification processes are not fool proof, and organisations should recognise that today’s “ordinary” data could become tomorrow’s sensitive information.

> A Desjardins Group rogue employee used his legitimate user credentials to steal around 2.9M records of customer account data. We must assume that DLP was in place, but it failed to detect this sensitive data export

Security Concerns

Mis-classification can lead to inappropriate security: As stated, documents classified as highly sensitive or confidential are sometimes secured by encryption. If this level of security is hard to use, people will avoid it. Staff will sometimes mis-classify documents simply because it's easier. Automated classification processes are only as good as the way they are configured. If files are not "discovered" they will not be classified, and therefore not appropriately secured. In addition, database files, temporary and log files are usually not classified though they often contain sensitive information. Many classification and rights management systems also only cater for commonly used file types, disregarding others completely. Why not assume that everything is sensitive? Then data security would be far simpler.

Resolving the Security Concerns

With SecureAge SecureData everything is encrypted, no matter what type of file, so it no longer matters – from an IT security perspective – whether data is classified correctly or not. SecureData is designed to be completely transparent to the user, who continues to operate in the way they would expect to work. With no performance degredation and no interference to applications, the data is strongly protected without bothering the user.

Database Encryption

Most commercial databases provide an option for encryption – normally Transparent Data Encryption (TDE). However, this is often expensive, version-specific and only encrypts the vendor's own databases, each with their own management system.

Data Breach Scenario

Database log or temporary files that contain sensitive information are copied to USB storage. These files, together with other unstructured files, are unprotected. Alternatively, a database is held in a cloud service but is mistakenly not securely configured. There are many media reports of cloud databases shown to be unprotected.

> Gekko Group – a leading European hotel booking platform – leaked over 1TB of data on customers, clients and partners thanks to an unsecured database, exposing them to account takeover, identity theft and financial fraud

Security Concerns

Theft of unstructured, temporary or log files: Most database applications store and manage unstructured files outside of the database. TDE does not encrypt these files. They also create temporary and log files which often contain sensitive information. These files are also not encrypted with TDE.

Theft of database files: If the data thief can access the files that constitute the database itself, and if the database is not encrypted, then the data can easily be stolen, reconstructed and accessed.

Resolving the Security Concerns

With SecureAge SecureData all databases, no matter which vendors, can be encrypted without impacting either the database or the application. Even during database operation, all data remains encrypted on disk so the threat of database file theft is mitigated.

Since SecureData implicitly encrypts all files regardless of type. All unstructured files, reports, logs and temporary files are automatically protected against data theft. Even data exported from a database and stored in local files will be encrypted so that stolen data is useless outside the organisation.

Encrypted Backups

Data backup technology routinely encrypts backup media or at least provides password protection. This secures data against backup media theft.

Data Breach Scenario

An administrator uses their “keys” to access confidential files within a backup. The backup media is encrypted, but the administrator holds the encryption keys and can therefore download unprotected files from the backups.

Security Concerns

Administrators can read backups: The administrator must know how to decrypt backups so that they can restore files when required. This means that it’s easy for the privileged user to gain access to, and steal files from a backup.

Resolving the Security Concerns

SecureAge SecureData encrypts all files at source, maintaining the encryption throughout a file’s lifecycle. This means that backups now contain encrypted files. If an administrator steals a file from such a backup, they will find that it is useless since it remains encrypted just for the authorised user.

> US radio giant Entercom reported that an unauthorised party was able to access database backup files stored in third-party cloud hosting services and containing Radio.com user credentials.
>
> Cathay Pacific’s £500K fine was in part due to the discovery that backup files were stored un-protected.

NIST Category 4
Information Protection Processes and Procedures

Cloud Services Security

Cloud services security consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. Cloud services are run by a third party, so you rely on that party to ensure your data is secure.

Data Breach Scenario

An administrator employed by the cloud services uses their privileged position to access and steal files within your storage bucket.

Security Concerns

Cloud service privileged users: Cloud security must prevent unauthorised external access as well as misuse by the third party’s privileged users. But you have no direct control over, or knowledge of those privileged users.

Resolving the Security Concerns

By encrypting data before it leaves your organisation’s systems, information is completely protected using SecureAge SecureData. Cloud admins may be able to see your files but they cannot access the data. And though mis-configured services, databases or infrastructure could lead to stolen files, the data inside them will be useless since it remains encrypted.

> 100 million Capital One customer records stored in AWS were stolen by an Amazon engineer who used a misconfigured firewall to gain remote access to 700+ folders of data. The on-going theft was not discovered for 4 months

NIST Category 5
Maintenance

Fundamental IT security advice advocates regular patching and maintenance of systems. This is of course excellent advice. By encrypting all files with SecureAge SecureData, even a server or desktop machine that is not fully up to date with security patches, and which has a vulnerability, will not enable the theft of useable data.

NIST Category 6
Protective Technology

Full Disk Encryption

BitLocker and similar systems encrypt the entire contents of a disk.

Security Concerns

As soon as a system that uses full disk encryption is running, all users and processes – legitimate and malicious – are given access to any file in the form of decrypted data. This means that full disk encryption is great for protecting data in a laptop that has been lost on a train, but has no security benefit for systems that are running.

Resolving the Security Concerns

SecureAge SecureData keeps files encrypted at all times – even while they're being accessed or edited. Only authorised individuals can decrypt this data while the system is running. And files copied to any other location remain encrypted.

SSL and TLS

SSL & TLS encrypt and secure data in transit. Most websites use this kind of security to ensure that anyone intercepting traffic is unable to access any useful data.

Security Concerns

As information is passed from the server to the client it is encrypted. Data held on the server, and any information stored on the client system is not protected by SSL/TLS.

Resolving the Security Concerns

With SecureAge SecureData, files are always encrypted. This means that they are protected not only in transit but also in use and at rest.

> Nedbank security breach involving 1.7M customer records at a third-party service provider. Though the data was sent to the third-party vial SSL/TLS, it was stored unencrypted

Anti-Malware

We rely on anti-malware systems to identify and kill off any “bad stuff”, so why is it that there are so many media reports of “successful” malware and ransomware attacks? Realising that anti-malware alone cannot block everything, organisations spend time and money educating their staff about cyber security and on the perils of clicking on, or opening anything that could be malicious.

Data Breach Scenario

A hacker – or insider – successfully deploys malware on your network, opening a backdoor.

Malware has been shown to evade corporate defences or to make use of the victim’s privileges. Either way, data access is achieved, and file exfiltration is straight forward.

Security Concerns

Malware is at least one step ahead: Ransomware has evolved into the Advanced Persistent Threat (APT), and now we have “disruptionware” which attempts to damage an organisation today, and continue to extort money into the future.

> Norske Hydro’s ransomware attack suffered around £60M costs due to recovery after being locked out of their systems. Had SecureAPlus been installed the malware would not have been allowed to execute so the perpetrators would not have been able to damage any IT services

Using zero-day attacks and machine learning techniques, hackers remain several steps ahead of anti-malware products. The traditional approach of attempting to recognise malware or to identify malicious behaviour in progress will always have the potential to let something through.

Resolving the Security Concerns

Because SecureAge SecureData keeps all data files encrypted at all times, any malware that attempts to steal data will exfiltrate only encrypted information. Once outside the organisation this data is useless to the thief. At this point we should again note SecureAge’s SecureAPlus which uses whitelisting and application control to block all unauthorised processes. This completely evades the malware problem by not allowing it to execute.

Conclusion

We've discussed commonly used IT security technologies within the categories of a cyber security framework and have seen that even with multiple layers of technology protecting data we still see successful data thefts. If the perpetrator – external or insider – can evade these defences then the information within stolen files is completely unprotected.

By encrypting every data file, no matter where it is stored, SecureAge augments existing cyber security layers by inherently and invisibly encrypting the data itself, making it useless once stolen. Making stolen data useless outside the organisation mitigates the devastation of a data breach – regulatory, brand damage, legal, business recovery, etc. The SecureAge approach ensures that sensitive and confidential information is not compromised.

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 whitelisting 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 & 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

To see more of our whitepapers click here. Please get in touch to find out more about SecureAge's enterprise data security solutions. We're happy to discuss how we can improve your data security and arrange a free trial: contact us.

Website www.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