5 KEYS ☑ 🔒 ☑ to secure INFORMATION MANAGEMENT

It seems data breaches have become a permanent part of reality in modern information management, disrupting business operations and leading to exposure of business and customer data. A study by Gemalto estimates that in 2016, over 1.3 billion records were lost in data breaches.[1] While the few high-profile exposures of major retailers and service providers received most attention in the press, many more breaches at smaller and lesser-known companies and organizations contributed to the statistic. This underscores the fact that "security by obscurity" is no longer a viable strategy for information management. Smaller, less protected companies and organizations are prime targets for hackers, and these breaches are also more likely to go undetected and unreported.

The threat landscape has changed dramatically over the last decade. Sophisticated and highly automated hacking tools are now widely available, lowering the barrier to entry and contributing to the proliferation of hackers. But forget the Hollywood image of hackers. Most common breaches today are not cases of industrial and international espionage. Hacking has become a volume business with a rather mundane objective: To plunder caches of personal information of average people.

... in 2016, **over 1.3 billion** records were lost in data breaches

This personally identifiable information (PII) can be email addresses, website logons, social security numbers, bank and credit card accounts and health insurance information. From colleges and hospitals to banks and insurance companies, this type of customer information is core to many business operations, but is often not very well-protected. When this information is captured, used and stored without proper security considerations, the organization and its customers are exposed to undue risk that can result in fines, litigation and loss of customers.

[1] Gemalto. Findings from 2016 Breach Level Index. 2017

Securing information management

Information management solutions are instrumental in customer onboarding, transaction processing and case management. They are core business technology engines that enable the capture of this personal information and its delivery to the people, processes and systems that need it.

> With so much confidential data passing through today's business systems, modern information management solutions must be **expected to stand up to a higher degree of scrutiny** when it comes to data security.

The following five keys will help you select a vendor and the solution that will help secure your valuable business and customer data rather than introduce new risks and vulnerabilities into your organization.

1 PROTECTING DATA AT EVERY STATE

In today's information-driven organizations, data usually exists and needs to be protected in multiple states at any given time.

DATA AT REST

Your document scanning software and import solution will ingest documents and save them to a file server. If these documents contain confidential financial or personal information, your information management solution should have the ability to encrypt these files. While full disk encryption is a great layer in a robust security defense, it only protects you from the threat of hard disk theft. Once the server is powered on and the disk is decrypted, it is not encrypted again until shutdown. Since most file servers need to be online and available 24/7, those files are at risk.

OnBase by Hyland overcomes this limitation of full disk encryption with its encrypted disk groups module. OnBase offers customers the ability to keep files encrypted until users with the correct security permissions need to access them.

Another key to securing data at rest is password management. Passwords can grant access to confidential information, so be sure to confirm with your vendor how they store and manage passwords in their database. OnBase is pre-configured by default with medium security password policy, and protects passwords by encrypting them with the industry-recognized PBKDF2 password hashing algorithm. A pre-configured high security password policy is also available.

DATA IN TRANSIT

We live in an era of increasing connectivity. Business processes mandate that documents move from scanner to file server, to application server, to workstation, to tablet, to printer, to mobile phone and beyond. As your information moves from one system or device to another, it is at risk of being intercepted and captured, without your knowledge, by a malicious individual or application.

> As your information moves from one system or device to another, it is **at risk of being intercepted and captured**

This is why it is critical that your content is protected in transit. Ask your prospective vendor how they secure content as it moves throughout your network. OnBase leverages robust transport layer security (TLS) to encrypt data in transit, ensuring that it is unusable if intercepted by an attacker or unauthorized individual.

DATA IN USE

It is critical to also secure data when it is being accessed by your users. Modern organizations manage a wide range of data across numerous departments. Ensuring that only authorized users have access to sensitive information is not a trivial task. Ask your prospective vendor how their solution will help you secure data in use.

OnBase secures data in use at multiple levels:

- Comprehensive security policies with granular controls enable access security that complies with industry standards and regulations
- Dynamic data masking and redaction offer an additional layer of security within documents
- Customizable timeout settings provide the ability to log out users in case of inactivity

2 HAVING SECURE DEFAULTS, RIGHT OUT OF THE BOX

Some vendors provide security features but bury them in the administrative options. This is especially common in one-size-fits-all solutions, where the vendor leaves it to the customer to enable and configure all of their own security features. This may sound like good flexibility to have, but in reality it places undue burden on your business system administrators to learn advanced configuration and configure your solution to meet industry standards.

Not having the fundamental security features enabled and configured out of the box **ultimately places your data and systems at risk.**

Ask your prospective vendor what security features come enabled and pre-configured with your solution.

OnBase solutions come with security features enabled, providing security models that are based on the best practices, standards and regulations for your industry.

3 ENABLING USERS WITHOUT COMPROMISING SECURITY

Even with the most advanced intrusion detection and prevention technologies in place, your employees will continue to be one of the largest vulnerabilities in your security infrastructure. As organizations become increasingly data-driven, your employees need access to more systems and data sources. However, expanding regulation and compliance requirements demand increasing controls on how this data is accessed and used. Ultimately, your people strive to do their jobs effectively and efficiently, but imposing excessive security policies and procedures hinders their productivity and increases risk of non-compliance.

... your employees will continue to be **one of the largest vulnerabilities** in your security infrastructure

Your information management solution should be a key to solving this security puzzle by intelligently managing access controls and giving users the information they need to get their jobs done without compromising security.

OnBase is built around the concept of secure, role-based access to information. The security controls are designed to limit user permissions to the bare minimum that they need in order to do their job. Following the "Principle of Least Privilege," this approach minimizes the risk of intentional or unintentional exposure without hindering the user's productivity.

4 PROTECTING AGAINST VULNERABILITIES

Modern software is incredibly complex, and often includes modules from dozens of various sources. It is the vendor's responsibility to track any potential vulnerabilities across the entire solution and proactively update or fix any modules that are discovered to be vulnerable. Organizations like Open Web Application Security Project (OWASP) track vulnerability data for common software packages that may be used by multiple vendors in their own software. (OWASP even publishes a Top 10 list of most critical application security risks). Ask your prospective vendor how they track and test for vulnerabilities in their product.

OnBase and other solutions from Hyland benefit from internal development and quality assurance staff who track and address any potential vulnerabilities and exploits, including the ones highlighted in the OWASP Top 10 List. Additionally, Hyland utilizes secure development practices, automated security scanning and manual penetration testing to continually test and secure solutions against a wide range of attacks.

5 ENSURING SECURITY IS NOT SKIN DEEP

Responsible software development companies don't treat security as an afterthought. When it comes to secure information management, *how* software is developed is just as important as the finished product. To truly commit to protecting your data, the vendor must implement security principles and tasks at each phase in the product lifecycle, including development, testing and support. Ask your prospective vendor to describe the role of security at each phase in their product lifecycle.

> When it comes to secure information management, ***how*** software is developed is just as important as the finished product

To protect your data and systems, Hyland follows a strict Security Development Lifecycle methodology. This ensures specific security tasks at every stage of product development and testing, and quality assurance. Hyland also trains all development and quality assurance employees on the skills and tools needed to prevent and detect software vulnerabilities.

Ready to elevate your security?

The right information management solution should help you reduce risk and improve regulatory compliance, instead of introducing new risks and vulnerabilities.

DOWNLOAD NOW: Choose a Secure Information Management Solution

Download this worksheet to help you in your selection process.

ABOUT ONBASE BY HYLAND

OnBase is a single enterprise information platform for managing content, processes and cases deployed on-premises or in the **Hyland Cloud**. Providing enterprise content management (ECM), case management, business process management (BPM), records management and capture all on a single platform, OnBase transforms organizations around the globe by empowering them to become more agile, efficient and effective. Enterprise cloud-based sharing capability for the OnBase platform is available with our complementary offering, **ShareBase by Hyland**.

To learn more, visit **OnBase.com/Security »**

OnBase® by Hyland