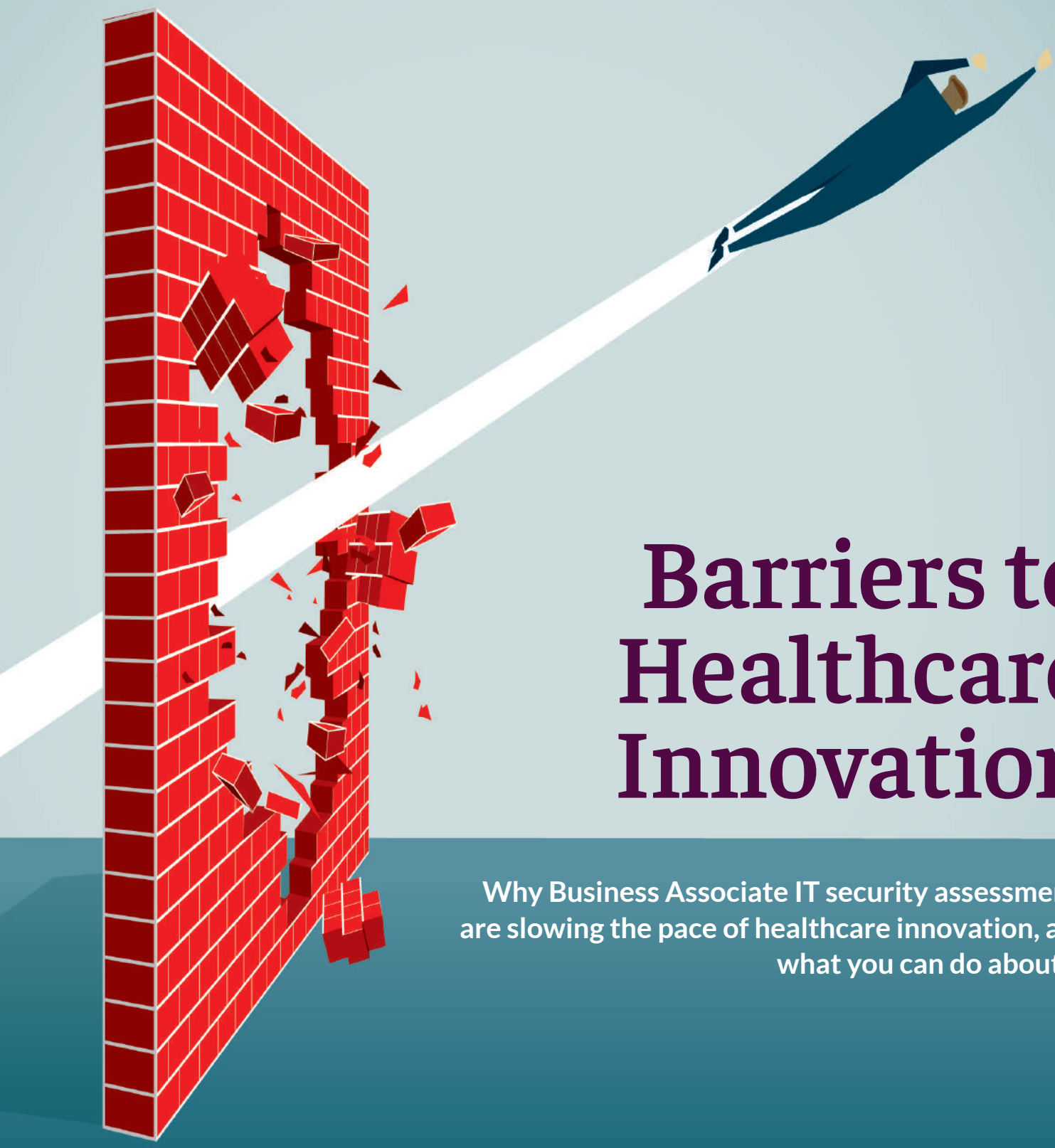
Datafy



Barriers to Healthcare Innovation

Why Business Associate IT security assessments are slowing the pace of healthcare innovation, and what you can do about it.

Barriers to Healthcare Innovation

The Business Associate IT Security Assessment

All of us who work in healthcare know that there are many barriers that prevent great ideas from getting to market. The AMA estimates that it takes 23 months on average for a new technology to be deployed in a healthcare system. In that time period, hospitals and their vendors negotiate terms, discuss integration, coordinate implementation and go through a lengthy IT security assessment process. Often an important and mandatory requirement of every new vendor relationship, existing

23 Number of months on average for a new technology to be deployed in a health system

IT security assessment processes are overly complex, burdensome and highly inefficient. This complexity impacts the entire healthcare ecosystem, stifling growth and inhibiting innovation, which ultimately can delay improved patient outcomes.

WHY KEEP READING?

In this white paper, we'll explore the role of the vendor IT security assessment as part of the hospital-vendor relationship and its importance to patients as well as the healthcare industry as a whole. We'll look at the pros and cons of current methods that hospitals are using to assess vendors and also ways to accelerate this collaborative process to help lifesaving advancements get to market faster.

Working Together is the Fundamental Principle

Simply stated, the IT security assessment is an important mechanism used to protect patient privacy. Hospitals, payers, providers, pharmaceuticals and other healthcare organizations designated as Covered Entities (CE) often set the technology standards that a vendor must meet in order to qualify to work with them. Whether it is connecting remotely to their systems, placing hardware or software inside the hospitals or exchanging data between the parties, it is imperative that the CE has a thorough understanding of and comfort with the vendor's security controls in situations where patient data is involved.

Additionally, vendor assessments provide hospitals with a full picture of their data security risks. HIPAA requires hospitals and other Covered Entities to maintain a legal contract between a hospital and a vendor, otherwise known as a business associate agreement (BAA), and to perform an overall risk assessment. It is considered a best practice to include all partner vendors in that assessment, as failure to adequately control vendor risk can lead to a breach of sensitive patient data, associated monetary penalties and reputational damage for both the hospital and the vendor.

20 Percent of healthcare data breaches that occurred at the vendor level in 2018

In 2018, third-party vendors accounted for over 20 percent of healthcare related data breaches[1]. This included Virtua Medical Group, which was fined $418,000 for a HIPAA breach that occurred at one of its vendors[2]. It is incidents like these that make the need for hospitals to thoroughly vet their partners abundantly clear.

[1] https://healthitsecurity.com/news/third-party-vendors-behind-20-of-healthcare-data-breaches-in-2018
[2] https://nj.gov/oag/newsreleases18/pr20180404b.html

A Highly Complex Problem

The sheer complexity of the process can be felt across the entire healthcare ecosystem and impacts stakeholders at all levels. From the provider's perspective, inefficiencies cause an overabundance of back and forth communication between different departments, including the technology team, the security team, the CISO's office, legal and the corresponding people within the vendor's organization. The problem is magnified when hospitals have to assess hundreds of vendors a year. These activities weigh heavily on hospital resources that are often stretched thin to begin with, and can discourage staff from focusing on this important issue.

IT assessments are equally challenging for those healthcare vendors who are an integral part of the patient care ecosystem. Burdened with having to respond to individual assessment questionnaires from each hospital, vendors ranging from software providers to hardware and infrastructure suppliers often struggle with basic understanding of the questions, how they pertain to their specific organizations and how to substantiate their responses. These assessments have financial implications as well, as employee costs, legal fees and management time all add up as the process draws out. The process can be so burdensome that it could discourage entrepreneurs from even pursuing a pilot or clinical trial.

Hospitals and their vendors are not the only parties affected. Patients have, perhaps, the most important stake in the game. With the value of stolen patient data rising on the black market, patients are increasingly becoming victims. It is up to the hospitals to take all reasonable efforts to protect patient data both within the confines of the hospital and when that information is shared with a third-party.

A System To Connect All Parties

While annual data privacy assessments are necessary, a system that is structured to work well for payers, providers and healthcare vendors alike is vital. This is no easy task. The system has to connect all parties and facilitate the rapid flow of information. It has to provide transparency about vulnerabilities so those issues can be addressed openly and solutions can be discussed. Assessment content (i.e., the questions asked of the vendors), has to be flexible, thorough, easy to update, relevant to the type of vendor being assessed and able to be tailored to an individual hospital's needs.

Identifying the Status Quo

In order to understand the landscape and get a high-level view of what measures are being taken to perform IT assessments, we spoke with hospitals, providers, health plans, government agencies, security experts and digital healthcare start-ups. What we found varied widely from organization to organization in both form and quality of the assessment. Our survey identified five general assessment formats – mostly spreadsheet or word document based, manual, lengthy and all were cumbersome and confusing. The following presents brief examples of each of the formats identified.

SHORT & LONG FORM DESCRIPTION BASED

These first two formats are very similar and are therefore grouped together. The most basic and unstructured of assessment formats, these short and long forms rely on the respondent to answer using a Word document or similar file. These formats rely on open ended questions that result in the respondent undertaking a free form writing exercise to convince the provider that they meet the necessary security standards. Inefficient for the vendors, these formats are equally challenging for the providers that send out hundreds of assessments a year and must read through each response.

The short form example shown below asks a series of brief questions broken up by topic. In some cases, the number of questions can reach into the hundreds. This format places the responsibility of interpreting the meaning of the questions with the respondent as instructions are often not provided. This format gives hospitals brief answers which do not always provide the depth of information they need to understand the vendor's security operations.

Account Management

- Who is authorized to request accounts?
- How are accouts requested?
- How are accounts created?

The longer form, shown below provides for more specific questions and answers. However, the vendor is also required to respond in a lengthy unstructured narrative fashion.

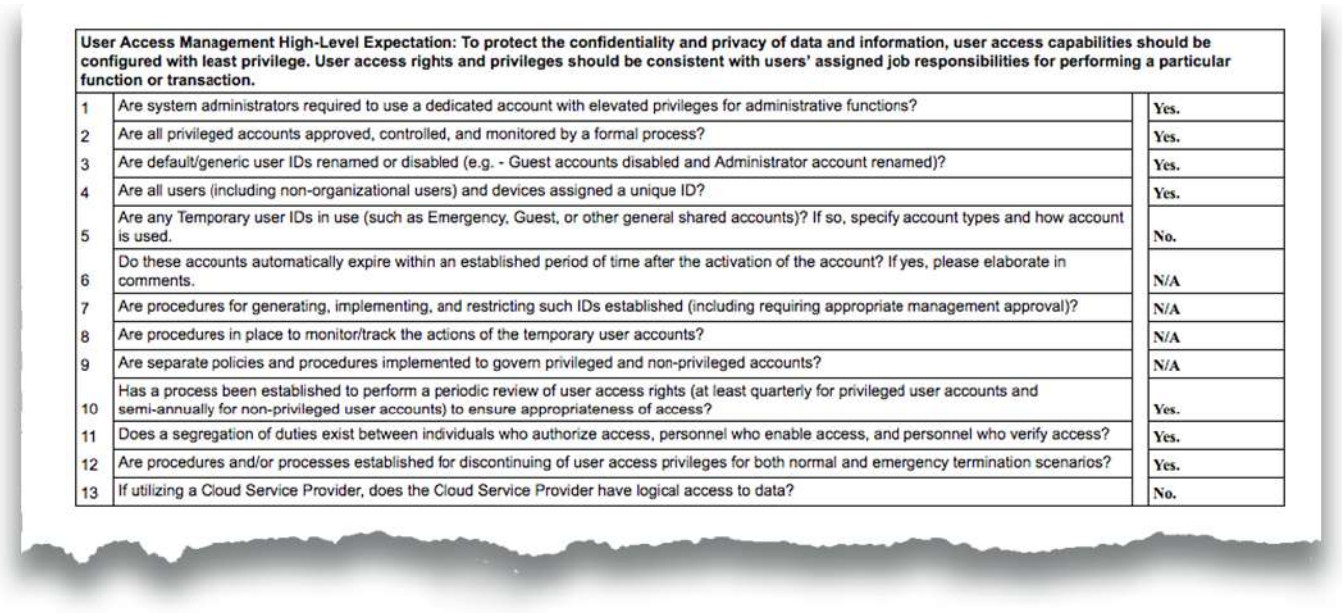
Access Controls

Describe the technical, operational and management controls used to provision access to system and data. Include how user accounts, privileged access and access to data are managed for an employee.

Information provided by the vendors to the hospital using these short and long forms is unstructured and significantly different from vendor to vendor. This highly unstructured format limits the hospital's ability to compare responses across companies and to establish standards. Additionally, given the disparity of assessment results, this method tends to encourage unnecessary back and forth between the hospital and the Business Associate.

YES or NO FORMAT

The most common format observed, this questionnaire presents the vendor with a long list of questions prompting a Yes, No or N/A reply. The questionnaires observed averaged around 300 questions, but some, typically from pharmaceutical companies, could be twice as long. While this questionnaire format may be faster to answer as compared to the short and long versions, matters of data security, policies, procedures and administrative tasks are often not as black and white as a Yes/No answer can capture. Additionally, the simplicity of this question format can easily lead the respondent to answer "Yes" in many cases where a "No" is more appropriate to avoid lengthy explanations.



	User Access Management High-Level Expectation: To protect the confidentiality and privacy of data and information, user access capabilities should be configured with least privilege. User access rights and privileges should be consistent with users' assigned job responsibilities for performing a particular function or transaction.	
1	Are system administrators required to use a dedicated account with elevated privileges for administrative functions?	Yes.
2	Are all privileged accounts approved, controlled, and monitored by a formal process?	Yes.
3	Are default/generic user IDs renamed or disabled (e.g. - Guest accounts disabled and Administrator account renamed)?	Yes.
4	Are all users (including non-organizational users) and devices assigned a unique ID?	Yes.
5	Are any Temporary user IDs in use (such as Emergency, Guest, or other general shared accounts)? If so, specify account types and how account is used.	No.
6	Do these accounts automatically expire within an established period of time after the activation of the account? If yes, please elaborate in comments.	N/A
7	Are procedures for generating, implementing, and restricting such IDs established (including requiring appropriate management approval)?	N/A
8	Are procedures in place to monitor/track the actions of the temporary user accounts?	N/A
9	Are separate policies and procedures implemented to govern privileged and non-privileged accounts?	N/A
10	Has a process been established to perform a periodic review of user access rights (at least quarterly for privileged user accounts and semi-annually for non-privileged user accounts) to ensure appropriateness of access?	Yes.
11	Does a segregation of duties exist between individuals who authorize access, personnel who enable access, and personnel who verify access?	Yes.
12	Are procedures and/or processes established for discontinuing of user access privileges for both normal and emergency termination scenarios?	Yes.
13	If utilizing a Cloud Service Provider, does the Cloud Service Provider have logical access to data?	No.

SCALE BASED

The scale based questionnaire reaches a little farther than the three previous formats. This template seeks to create a scale of points based on predetermined answers ranging from least acceptable to most acceptable. Here we see the first example of a questionnaire providing a level of explanation to help the respondent in answering. However, the construct of filling in numeric answers based on the scale provided, makes it very difficult to drill into detail and to confirm accuracy.

Evaluation Criteria	Criteria Explanation	Scale Explanation	Vendor Current State
Identity and access management	Facility for defining, administering, and tracking priviledges accross corporate systems	0= The organization has no coherent identity and access management process or tools. 1= The organization employs basic access control and provisioning systems for some IT assets. 2= The organization employes formal access controls and provisionning systems for Key IT assets. 3= The organization has defined user priviledges based on job function, with well-defined access policies and provisioning proesses. 4= The organization closely monitors user access to identify policy violations and continuously improves its access management processes to reduce risk. 5= The organization features close collaboration between the security department and business to optimize effectiveness and efficiency of the access control and provisioning functions.	
Federated Access Control		Do you support federated access control (SAML)?	

MATURITY BASED

The maturity based model is the most complex questionnaire identified. This format presents a list of steps that describe a company's technology operations. The addition of a basic scoring methodology gives the hospital a minimum level of quantitative data about the vendor, but in this case the numerical score likely just guides the hospital's review of the questionnaire. This scoring methodology has many deficiencies, including how the most desirable answers contribute to higher score, and, like the Yes/No format, may encourage the respondent to favor the "better" answers.

					60%	10%	10%	5%	10%	5%		
Control	Requirement Identifier		Requirement	Assessment Question	...self-attest compliance with this requirement?	...address this requirement in the MSA?	....provide policies and procedures for inspection?	...allow technical inspection?	....use a 3rd party service to independently verify compliance?	....provide evidence of continuous monitoring and operational compliance?	Combined Score	Grade
Identity & Access Management User ID Credentials	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?							0%	F
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?							0%	F
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?							0%	F
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?							0%	F
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?							0%	F
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?							0%	F
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?							0%	F
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?							0%	F
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?							0%	F
		IAM-12.10		Do you support the ability to force password changes upon first logon?							0%	F
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?							0%	F

Complexity Prevents Compliance

While the hospitals we spoke to that have a vendor assessment program tend to use one of the above methods, we found many more do not have a program in place at all. These hospitals cite non-standardization, the difficulty of adopting and maintaining an appropriate vendor IT security program, cost and competing priorities as barriers preventing hospital IT departments from deploying a program.

Conclusion

Each day we seek new and innovative ways to improve patient care. However, significant barriers exist which prevent these innovations from getting to market. One such barrier is the vendor IT security assessment. This complex process impacts everyone from hospital staff and healthcare product and service providers to patients. Variability across the industry contributes to both hospital staff and their business associates spending a great deal of time and money just to establish the basic levels of trust needed to work together and, most importantly, to protect patient data. Streamlining the vendor IT security assessment barrier will benefit the entire healthcare system and empower innovators and providers to bring life-saving advancements to market.

THE DATAFY SOLUTION

Datafy enables the security assessment process across the entire healthcare ecosystem, speeding time-to-market and facilitating the collaboration that fosters life saving innovation.

This SaaS platform was developed to alleviate the burden of manually managing vendor compliance. Its sophisticated design replaces the commonplace spreadsheet questionnaire with an interactive and powerful interface that speeds response times and increases accuracy of gathered information.

FOR INFORMATION: info@datafy.health or **212-403-7000**