

HOW TO CREATE A SECURITY-FIRST ORGANIZATION

Organizations invest a great amount of resources to meet industry and government regulations that will help them spot the gaps in their data security. Yet, some organizations still fall victim to a data breach, despite meeting all industry and government compliance checks. When this happens, it's likely that the organization was more focused on avoiding penalties and being "compliance first" than on developing a strong cybersecurity program.

Use this workable document as your first step to becoming a "security-first" organization by defining your role in security, gauging how you can achieve compliance, and selecting the right security-service provider for your organization.

DEFINE YOUR ROLE IN SECURITY

To get started, businesses must carefully weigh what security functions they are willing to take on and when, and how those decisions affect the ability to scale and grow. A brand-new "born in the cloud" startup may choose to outsource all their security functions to a third party who has the scale and expertise to protect their organization at a reasonable cost. A larger company may have dedicated security staff in place and prefer to maintain a blend of internal security operations while leveraging third-party tools for analysis of incidents and subsequent alerting on areas of concern.

Utilize these guestions when establishing and optimizing your security program as you scale.

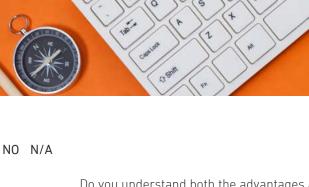
YES NO N/A

Do you understand the Shared Responsibility Model and what your organization is responsible for in respect to security?

Is your organization subject to any compliance frameworks? If so, do you understand how to address security controls for your workloads in the cloud?

Do you understand the various native tools and capabilities the cloud service provider offers that can help you secure your applications and data?





YES NO N/A Do you understand both the advantages and limitations of these tools? Have you identified additional security capabilities your organization will need to effectively secure your applications and data? How does your organization plan to perform vulnerability scanning? What will be the program for patching applications and systems to address vulnerabilities? If you have or expect to have a blended on-premise, hosted, and/or cloud environment, have you identified ways to unify security and visibility across that entire environment? Who is going to monitor activity and alerting?

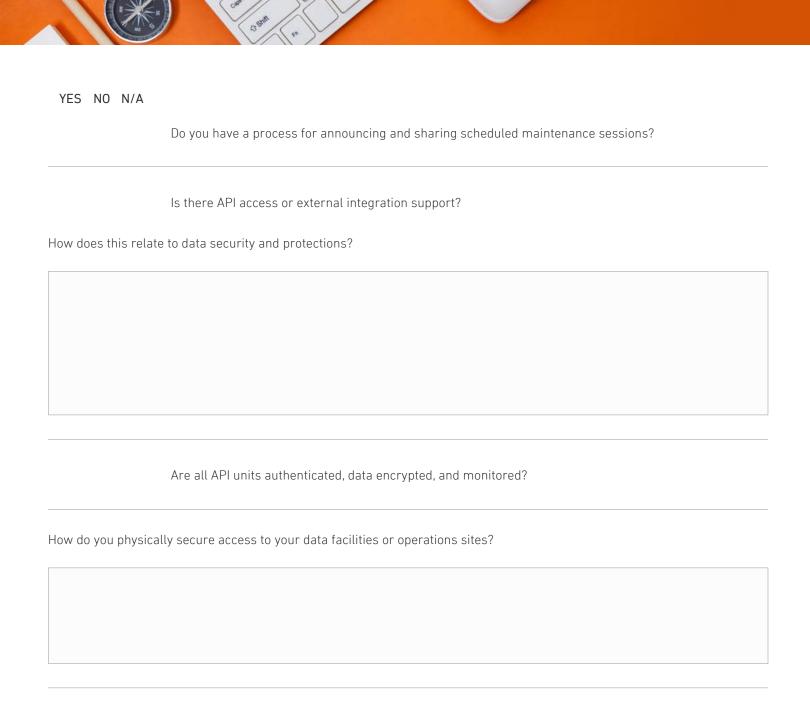


Who will be respon	sible for the review and investigation of al	erts and determine how to respond and/or remediate them?		
Who will be respon	sible for ongoing tuning and optimization o	of your security operations?		
ACHIEVE	COMPLIANCE			
level of compliance		thcare, retail, and financial industries, must comply with a certain is it pertains to data breach notification. No matter the regulation, by is in passing an audit.		
YES NO N/A				
	Do you have a corporate security policy	?		
	Is there a dedicated security team in pla	ace to handle events and failures?		
	Do you have a formal procedure for reporting a security violation or data breach?			
	Do you regularly conduct penetration te	sting or have a third party handle the process?		
lf so, when was the and what were the	last relevant test performed, results?	What are you doing to remedy any flaws or vulnerabilities discovered?		



Whether through external means or internal discovery, what are you doing to both identify and remediate vulnerabilities in your system and network?
How often are applications or software tools updated?
What is the process for doing so, and how does this affect security?
What about customer or client downtime?
How long will the update process take?
What is the process for doing so, and how does this affect security? What about customer or client downtime?





Do you have documentation to support this?

How do you comply with HIPAA, Sarbanes-Oxley, PCI DSS 3.0, GDPR, and other similar-level regulations?





YES NO N/A

Are all your processes, including data backups, documented in full with details on how you handle operations?

	_			
How far does your disaster recovery plan extend?				
What will you do if your customers are affected by a breach?				
How will you continue to ensure their privacy and security?				



SELECT A SECURITY PROVIDER

For businesses looking to security-service providers to help them secure their sensitive applications and data, not all providers are created equal. Leverage these questions in any discussions with third-party, security-service providers to determine how their offerings will fit within your current program.

YES NO N/A

Is the provider able to unify security across your full environment (cloud, on-premise, hosted, etc.) or just one area?

or just one area.
How do the provider's offerings and roadmap address any requirements your organization may have for security across a 2-year horizon?
Does the provider require deployment of hardware into your environment?
If so, how difficult is implementation, and how long will implementation take versus a software-based solution?



What is the division of responsibilities between provider and customer?					
What specific aspects of ongoing security operations is the provider handling?					
YES NO N/A					
Will staff have access to the provider's security and compliance staff?					
Is billing fixed or does it allow for consumption-based billing, aka "pay only for what you use?"	Fixed Billing	Allowes for Cunsumption Based Billing			
How integrated are the underlying capabilities of the provider's solution?					

