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 questions 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?

Type your answer here.

What will be the program for patching applications and systems to address vulnerabilities?

Type your answer here.

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?

Type your answer here.

Who is going to monitor activity and alerting?

Type your answer here.

Who will be responsible for the review and investigation of alerts and determine how to respond and/or remediate them?

Type your answer here.

Who will be responsible for ongoing tuning and optimization of your security operations?

Type your answer here.

ACHIEVE COMPLIANCE

Most organizations, especially those who work with or in healthcare, retail, and financial industries, must comply with a certain level of compliance for data security and privacy–especially as it pertains to data breach notification. No matter the regulation, use the below questions to gauge how prepared your company is in passing an audit.

YES	NO	N/A	
○	○	○	Do you have a corporate security policy?
○	○	○	Is there a dedicated security team in place to handle events and failures?
○	○	○	Do you have a formal procedure for reporting a security violation or data breach?
○	○	○	Do you regularly conduct penetration testing or have a third party handle the process?

If so, when was the last relevant test performed, and what were the results?

Type your answer here.

What are you doing to remedy any flaws or vulnerabilities discovered?

Type your answer here.

Whether through external means or internal discovery, what are you doing to both identify and remediate vulnerabilities in your system and network?

Type your answer here.

How often are applications or software tools updated?

Type your answer here.

What is the process for doing so, and how does this affect security?

Type your answer here.

What about customer or client downtime?

Type your answer here.

How long will the update process take?

Type your answer here.

YES NO N/A

○ ○ ○ Do you have a process for announcing and sharing scheduled maintenance sessions?

○ ○ ○ Is there API access or external integration support?

How does this relate to data security and protections?

Type your answer here.

○ ○ ○ Are all API units authenticated, data encrypted, and monitored?

How do you physically secure access to your data facilities or operations sites?

Type your answer here.

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

Type your answer here.

○ ○ ○ Do you have documentation to support this?

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?

Type your answer here.

What will you do if your customers are affected by a breach?

Type your answer here.

How will you continue to ensure their privacy and security?

Type your answer here.

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?

How do the provider's offerings and roadmap address any requirements your organization may have for security across a 2-year horizon?

Type your answer here.

○	○	○	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?

Type your answer here.

What is the division of responsibilities between provider and customer?

Type your answer here.

What specific aspects of ongoing security operations is the provider handling?

Type your answer here.

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?

Type your answer here.

|