SECURITY&COMPLIANCE

FOR REGIONAL BANKS AT A GLANCE

Financial institutions are more dependent than ever on the use of technology to conduct day-to-day business. While this has revolutionized the industry, it also opens up banking establishments to several costly security concerns. In fact, the banking industry incurred higher cybercrime costs than any other industry in 2019, averaging $18.3 million per firm[1].

Audits of a bank's IT infrastructure are critical to the safekeeping of not only their clients' personally identifiable information (PII), but their reputation as well. Even the most advanced IT environments can come up short on an audit.

Let's take a look at some of the most common weak spots that come up on IT audits and what can be done to correct them.

$18.3M

Average cybercrime costs per firm in the banking industry last year - higher than any other industry.

[1] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Identity and Access Management

Identity and access management pertains to the access levels of all user accounts created within a company network. Without a proper method for managing employee accounts, IT staff could unknowingly be handing off the keys to the kingdom to employees that aren't qualified.

Some of the most common pitfalls in identity and access management include neglecting to disable user accounts when employees separate from the company, high-level privileges being given to low-level employees, and a lack of employee password policies or their enforcement.

Patch Management

Hardware manufacturers typically develop software and OS-level patches meant to mitigate security concerns or software bugs. Failing to keep up with hardware and application patching levels can create holes in your environment that sophisticated hackers can easily penetrate. Some of the most common failed controls related to patch management include irregular patching schedules or neglecting them altogether.

Configuration Management

Having an understanding of all business systems and applications is critical to maintaining a healthy, secure environment.

A lack of configuration management protocols can lead to a lack of control over the infrastructure. This can result in rogue devices connecting to the internal network, unauthorized software being downloaded on employee workstations, and loopholes for cybersecurity attacks.

Lack of Internal Security Awareness Programs

Protecting business and client information is the responsibility of all employees, not just the IT team. Information about security initiatives should be shared with all staff to promote awareness of potential threats. Without the proper training programs in place, employees may unknowingly put the company at risk for cybersecurity attacks.

Response Steps Checklist

IDENTITY AND ACCESS MANAGEMENT

☐ Give the minimum level of access required for employees to do their job, reserving admin rights to senior IT staff only.

☐ Document standard levels of access based on job role.

☐ Implement standard operating procedures for disabling employee accounts after they separate from the company.

☐ Implement password policies that detail character count and complexity.

PATCH MANAGEMENT

☐ Develop a patching policy that outlines all systems to be patched and the frequency in which they will occur.

☐ Follow all manufacturer recommendations for patching frequency.

☐ Implement a small sample of patches as a control group for testing before implementing in your production environment.

CONFIGURATION MANAGEMENT

☐ Ensure only approved hardware solutions are implemented in the environment.

☐ Develop an approved list of software, and any requests for alternative software should be reviewed by the IT team before deployment.

☐ Local admin privileges should be removed from all workstations, reserving the ability to download software for IT staff only.

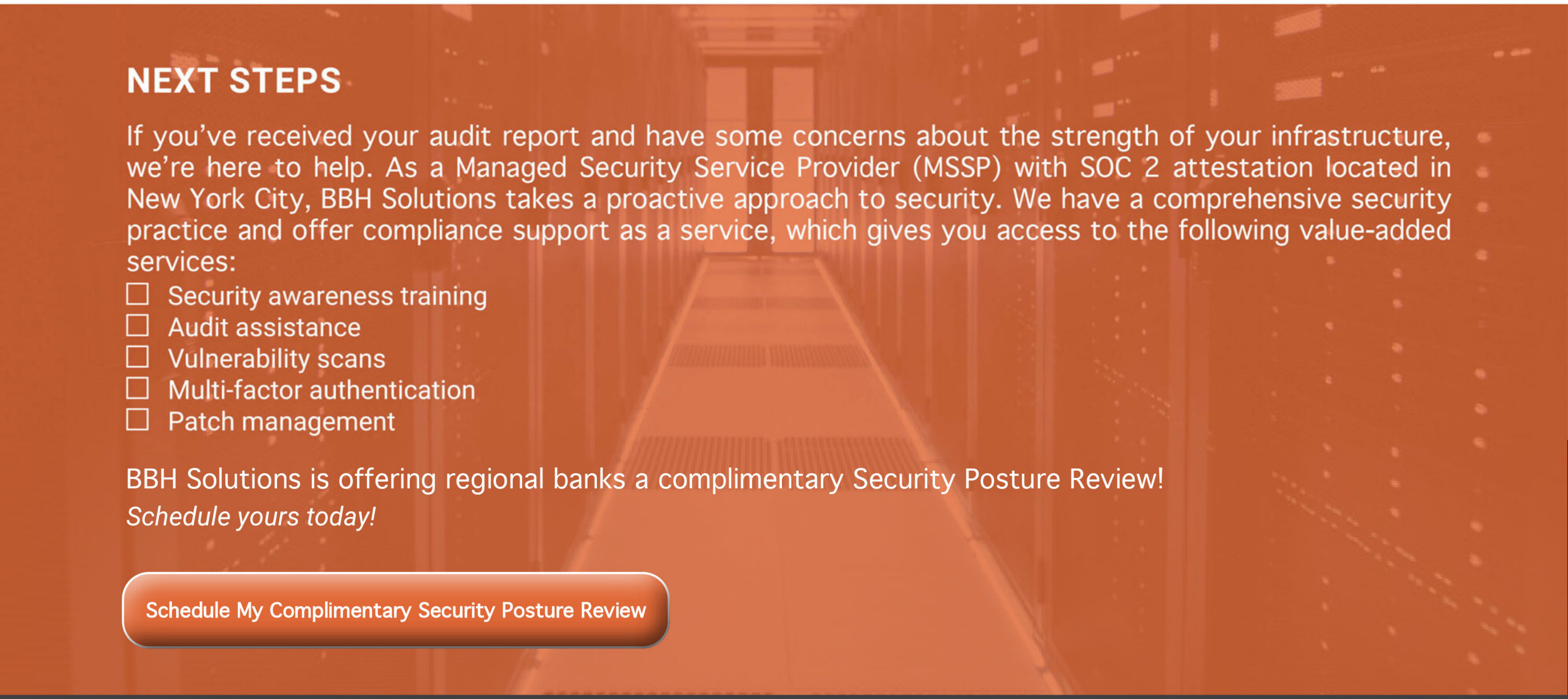
☐ Standard configurations for all equipment and applications should be documented and kept in a central repository.

☐ Configurations follow a cybersecurity framework standard, such as NIST or CIS.

SECURITY AWARENESS

☐ Communicate early and often with employees about security best practices.

☐ Conduct training on behaviors to avoid (clicking on embedded email links from senders they don't recognize, passing confidential information like account, credit card, or social security numbers via unencrypted email, utilizing weak passwords, etc.).



NEXT STEPS

If you've received your audit report and have some concerns about the strength of your infrastructure, we're here to help. As a Managed Security Service Provider (MSSP) with SOC 2 attestation located in New York City, BBH Solutions takes a proactive approach to security. We have a comprehensive security practice and offer compliance support as a service, which gives you access to the following value-added services:

☐ Security awareness training

☐ Audit assistance

☐ Vulnerability scans

☐ Multi-factor authentication

☐ Patch management

BBH Solutions is offering regional banks a complimentary Security Posture Review!

Schedule yours today!

Schedule My Complimentary Security Posture Review

AICPA SOC

NYBA

Microsoft Tier-1 Cloud Solutions Provider

CISCO Partner Premier Certified

bbhsolutions.com

BBH SOLUTIONS