NIST Cybersecurity & Risk Management

Case Study: Section 1.6 Self-Directed Exercise

Case Study Toolkit Resource

For this self-directed exercise, you will need to gather the resources below to complete the activity.

These resources will also be important for you to follow along with the case study for this course

- [ ] **NIST SP 800-37R2**
- [ ] **NIST CSF**
- [ ] **CSF Framework PDF: CSF Core Excel & CIS Controls**
- [ ] **PCI DSS**

NIST Cybersecurity & Risk Management

Case Study: Background

Set-up

Your firm has been hired to assess the security of a medium sized US-based accounting firm, RV&T.

Firm Background

RV&T is a family business covering basic bookkeeping to specialized wealth management. The firm has three office across the U.S., one East Coast in Atlanta, One Central in Dallas, and one West Coast in San Francisco. The firm has clients in 30 states, roughly split between the three

NIST Cybersecurity & Risk Management

geographies they operate offices in.

Personnel

30 tax accountants (10 per office)

6 salespeople (2 per office)

12 support personnel / management (4 per office)

3 IT system administrators (1 per office)

* Many of their personnel are remote workers.

RV&T utilizes a combination of on-premise and cloud-based infrastructure

Applications :

- Microsoft 365 (cloud based)

NIST Cybersecurity & Risk Management

- QuickBooks (hybrid solution)
- Salesforce (cloud based)
- Legacy application running on Windows Server 2016 with FTP (on-premises in each office)

Hardware:

- Every employee has a company issued laptop running Windows 10 Pro.
- The salespeople have an additional company issued tablet device (an iPad) running one generation prior to the latest iPad iOS for in person meetings and presentations.

NIST Cybersecurity & Risk Management

- The IT Administrators run one or more Virtual Machines (VMs) to allow them to have access to additional applications and O/Ss necessary for them to manage and maintain the on-premises infrastructure.
- The firm has a BYOD policy for mobile/smart devices and allows personally owned and enabled devices to be connected to corporate systems and to access corporate and client data.

NIST Cybersecurity & Risk Management

Security Infrastructure:

- Palo Alto Firewalls are in each office protecting all internal infrastructure.
- Trend Micro TippingPoint NGIPS is in place monitoring all network traffic for threats
- Logging for the legacy application running on Windows Server 2016 with FTP is handled locally on each server in each office

Current State of Operations

RV&T has adequate pre-existing cyber security measures in place, but they are

NIST Cybersecurity & Risk Management

concerned that with the ever changing regulatory landscape that they are treading water at best, and are looking for guidance on additional areas and controls that they might be overlooking.

The Challenge

RV&T handles a significant volume of confidential data for their clients, and are worried about the growing possibilities of being subjected to fines/penalties and /or legal action under new legislation. As a result they want to reduce any possible vulnerabilities they have and avoid any

NIST Cybersecurity & Risk Management

breaches or disclosures.

Given the recent roll-out of data-related legislation, they want to be sure they are exceeding their obligations to minimize risk. They have come to your firm with the intent to meet the current GDPR and California Consumer Privacy Act (CCPA) requirements.

The Policy Inventory

The following policies have been created and are in force currently:

- Bring Your Own Device (BYOD)
- Acceptable Use of I.T. resources and

NIST Cybersecurity & Risk Management

systems.

- Data Access
- Password Management
- E-Mail
- Social Media

NIST Cybersecurity & Risk Management

Case Study Interaction #3: Section #4

Set up:

Your firm has been hired to assess the security of a medium sized US-based accounting firm, RV&T.

Background:

- There have been some unusual events and activities occurring intermittently around the legacy application running on Windows Server 2016 with FTP (on-premises) in the Central office in Dallas.
- The system has been very slow to

respond to user requests for access at the beginning and end of each work day.

- The Task Manager on the Windows Server 2016 computer shows 90% memory and 90% CPU utilization during these periods upon review, but almost no network traffic.

Current State of Operations:

The Windows Server is configured to log only failed logon attempts locally to the security log.

NIST Cybersecurity & Risk Management

Use this page to write your responses

NIST Cybersecurity & Risk Management

Case Study Interaction #4: Section #8

Set up:

Your firm has been hired to assess the security of a medium sized US-based accounting firm, RV&T.

Background:

Among the many clients that the firm has across the U.S., there are several in each of the following verticals:

a. Health Care

b. Insurance

c. Retail (on-line & brick & mortar)

d. Banking

NIST Cybersecurity & Risk Management

These client verticals are all represented in each of the three regional offices that the firm currently maintains (The firm has three office across the U.S., one East Coast in Atlanta, One Central in Dallas, and one West Coast in San Francisco.)

Current State of Operations:

A pre-audit, conducted PRIOR to your firm being hired to assess the security of RV&T has shown several areas of concern vis-a-vis alignment with appropriate/adequate industry standards and best practices such as the use of Multi-Factor Authentication

NIST Cybersecurity & Risk Management

(MFA) on ALL company owned device assets. In addition, the gap analysis that was conducted on the current control environment found misalignment across the operational landscapes, both on-premises and cloud. The senior leadership of RV&T has grown increasingly concerned about these findings, in light of the increasing frequency of breaches and and ransomware attacks that are being successfully executed against organizations globally.

NIST Cybersecurity & Risk Management

Use this page to write your responses

NIST Cybersecurity & Risk Management

Case Study Interaction #5: Section #10

Set up:

Your firm has been hired to assess the security of a medium sized US-based accounting firm, RV&T.

Background:

Among the many clients that the firm has across the U.S., there are several in each of the following verticals:

a. Health Care

b. Insurance

c. Retail (on-line & brick & mortar)

d. Banking

NIST Cybersecurity & Risk Management

These client verticals are all represented in each of the three regional offices that the firm currently maintains (The firm has three office across the U.S., one East Coast in Atlanta, One Central in Dallas, and one West Coast in San Francisco.)

Current state of operations:

A pre-audit, conducted PRIOR to your firm being hired to assess the security of RV&T has shown several areas of concern vis-a-vis alignment with appropriate/adequate industry

NIST Cybersecurity & Risk Management

standards and best practices such as the use of Multi-Factor Authentication (MFA) on ALL company owned device assets. In addition, the gap analysis that was conducted on the current control environment found misalignment across the operational landscapes, both on-premises and cloud. The senior leadership of RV&T has grown increasingly concerned about these findings, in light of the increasing frequency of breaches and ransomware attacks that are being

NIST Cybersecurity & Risk Management

successfully executed against

organizations globally.

NIST Cybersecurity & Risk Management

Use this page to write your responses

NIST Cybersecurity & Risk Management

Case Study Interaction #6: Section #13

Using the case study:

- *What is/are the appropriate controls addressing system disposal for the legacy application server?*
- *What is/are the important systems that have to be updated as a result of the removal from service?*
- *Do any users and/or application owners need to be notified as a result of the removal from service?*

NIST Cybersecurity & Risk Management

- *What are the relevant federal laws, regulations, directives, policies, and /or standards that would have to be complied with as a result of the removal from service for the disposed system?*

NIST Cybersecurity & Risk Management

Use this page to write your responses