plante moran | Audit. Tax. Consulting. Wealth Management.

Vendor Management

Are You “Really” Managing Your Vendors, Or Are You Just “Checking a Box”?

Presenter

Colin Taggart

Colin.Taggart@plantemoran.com
248-223-3235

Agenda

- Understanding the Current Vendor Management Environment
  - Knowing your vendors and the current regulatory environment
- How to Build a Vendor Management Program That Provides Value
  - Vendor risk assessments, questionnaires and ongoing monitoring through the use of tools and reviews of SOC reports
- Vendor Management Takeaways
- Questions

Understanding the Current Vendor Management Environment

Know Your Vendors

Core processing system

Anti-money laundering, fraud detection systems

Loan origination and loan management systems

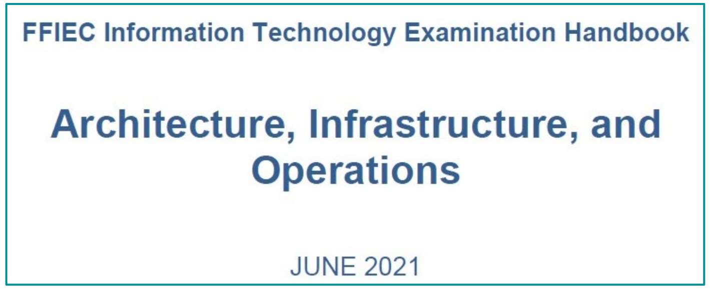
Website hosting and online banking systems

HR/payroll systems

Data warehouse

Audit firms

Regulatory Environment

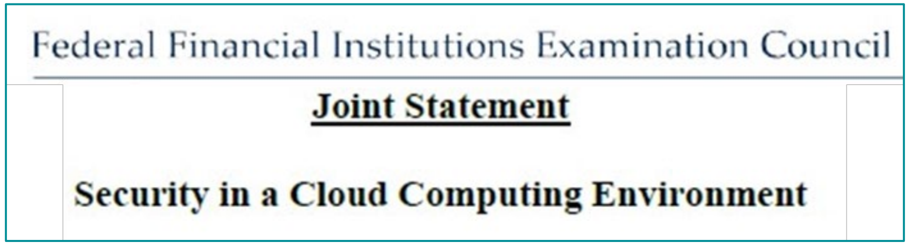


FFIEC Information Technology Examination Handbook

Architecture, Infrastructure, and Operations

JUNE 2021

"Third-party assurance reviews (e.g., SOC reviews, penetration tests, and vulnerability assessments) can provide an understanding of the cloud service provider's control environment and its ability to meet an entity's control expectations (e.g., compliance with applicable laws and regulations)."

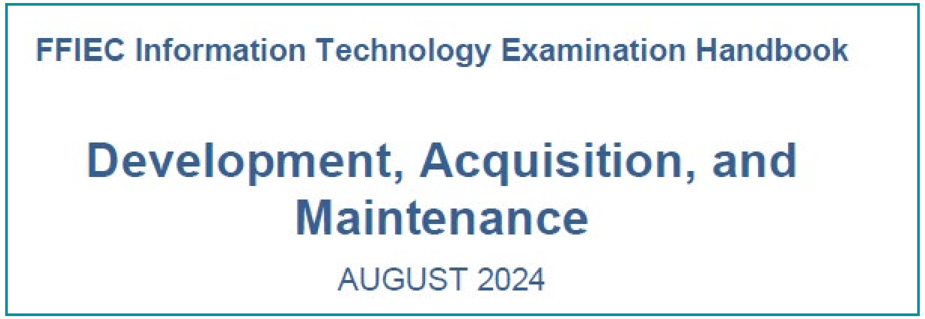


Federal Financial Institutions Examination Council

Joint Statement

Security in a Cloud Computing Environment

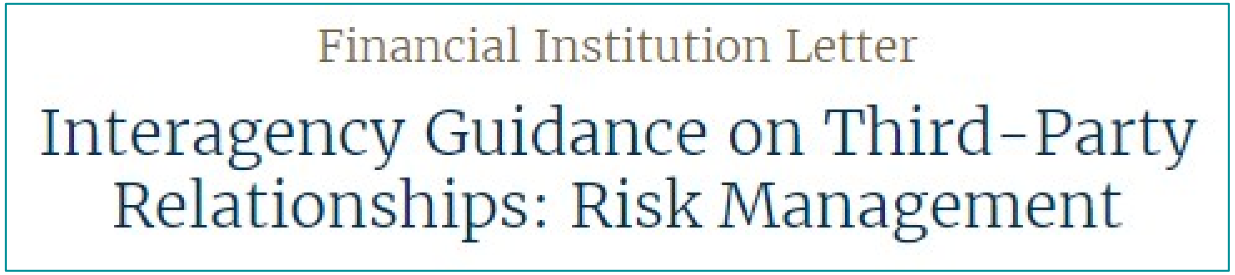
"As part of sound risk management, entities engage in more comprehensive and rigorous planning, due diligence, oversight, and management of third-party relationships that support higher-risk development, acquisition, and maintenance activities, including critical activities."



FFIEC Information Technology Examination Handbook

Development, Acquisition, and Maintenance

AUGUST 2024



Financial Institution Letter

Interagency Guidance on Third-Party Relationships: Risk Management

Third Parties – not just Vendors

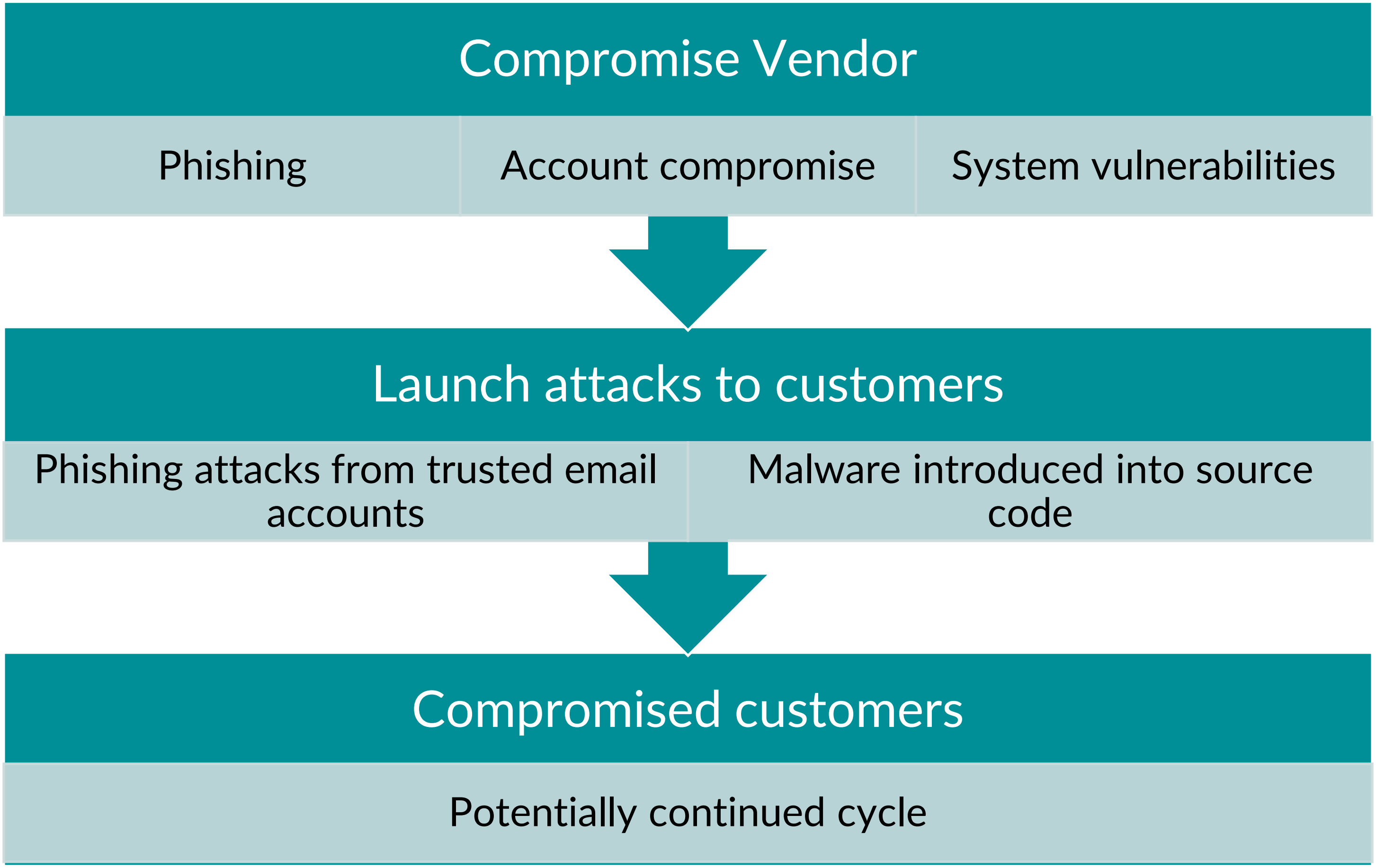
4th Party Risks

Board Oversight

Vendor Management Tools – Outsource Task, not Responsibility

Foreign Based Third Parties

Vendor Risks



Compromise Vendor

Phishing

Account compromise

System vulnerabilities

Launch attacks to customers

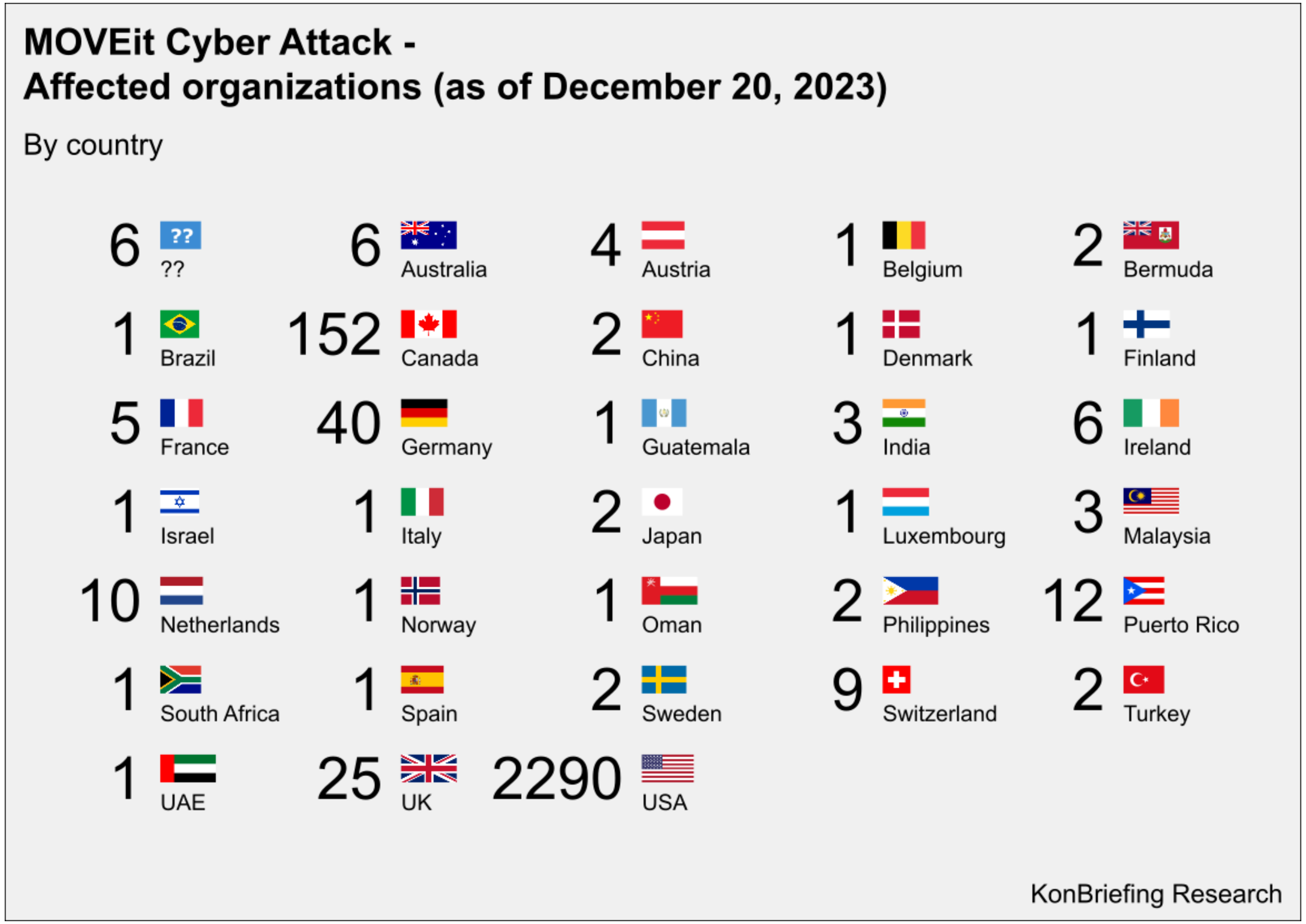
Phishing attacks from trusted email accounts

Malware introduced into source code

Compromised customers

Potentially continued cycle

MOVEit Zero Day Vulnerability



MOVEit Cyber Attack -
Affected organizations (as of December 20, 2023)

By country

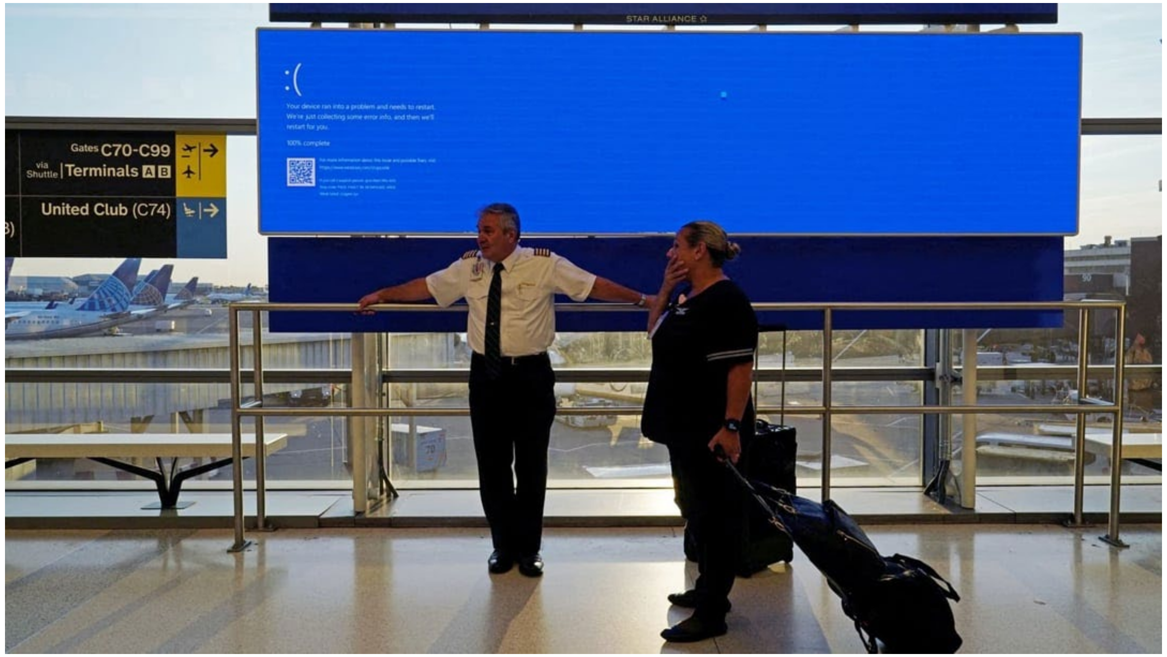
6	??	6	Australia	4	Austria	1	Belgium	2	Bermuda
1	Brazil	152	Canada	2	China	1	Denmark	1	Finland
5	France	40	Germany	1	Guatemala	3	India	6	Ireland
1	Israel	1	Italy	2	Japan	1	Luxembourg	3	Malaysia
10	Netherlands	1	Norway	1	Oman	2	Philippines	12	Puerto Rico
1	South Africa	1	Spain	2	Sweden	9	Switzerland	2	Turkey
1	UAE	25	UK	2290	USA				

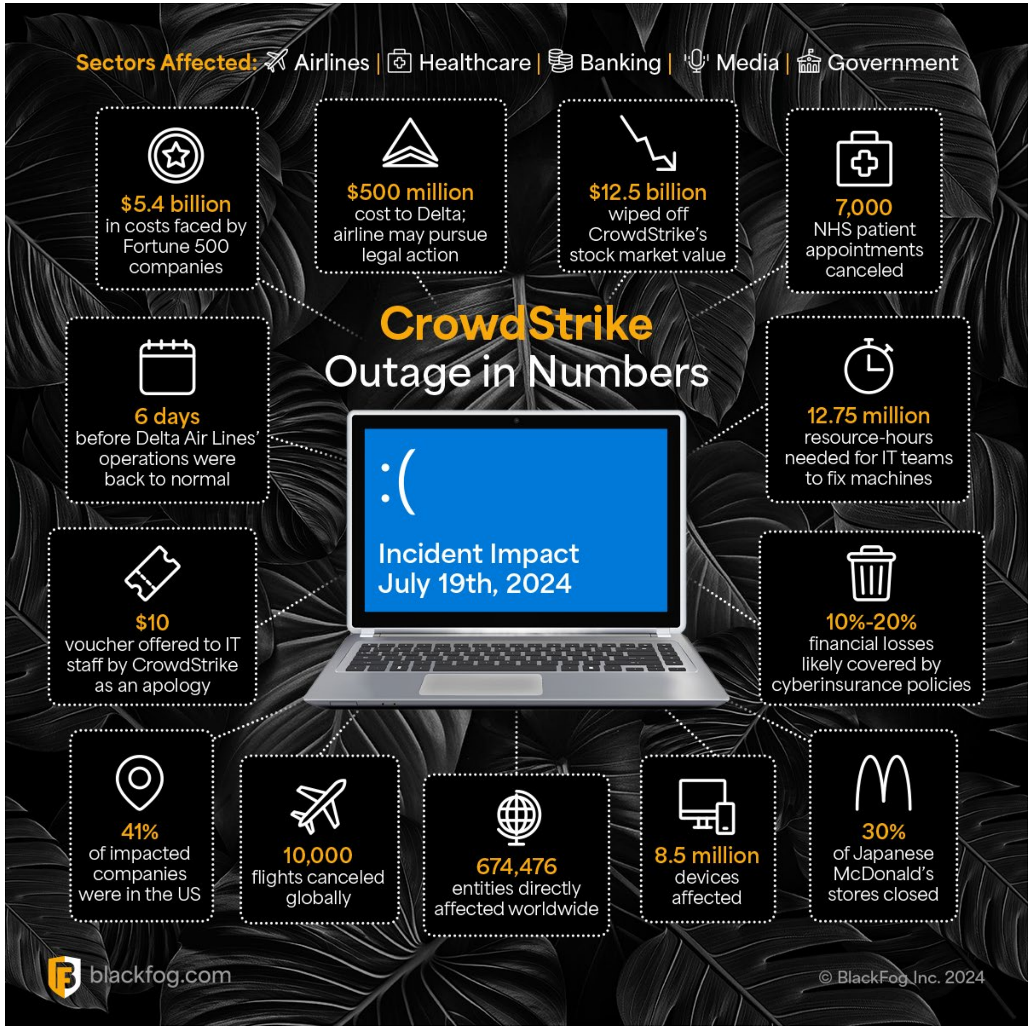
KonBriefing Research

2,700+ organizations

>94 million individuals

Lessons Learned from CrowdStrike





Sectors Affected: Airlines | Healthcare | Banking | Media | Government

$5.4 billion in costs faced by Fortune 500 companies

$500 million cost to Delta; airline may pursue legal action

$12.5 billion wiped off CrowdStrike's stock market value

7,000 NHS patient appointments canceled

CrowdStrike
Outage in Numbers

:(
Incident Impact
July 19th, 2024

6 days before Delta Air Lines' operations were back to normal

12.75 million resource-hours needed for IT teams to fix machines

$10 voucher offered to IT staff by CrowdStrike as an apology

10%-20% financial losses likely covered by cyberinsurance policies

41% of impacted companies were in the US

10,000 flights canceled globally

674,476 entities directly affected worldwide

8.5 million devices affected

30% of Japanese McDonald's stores closed

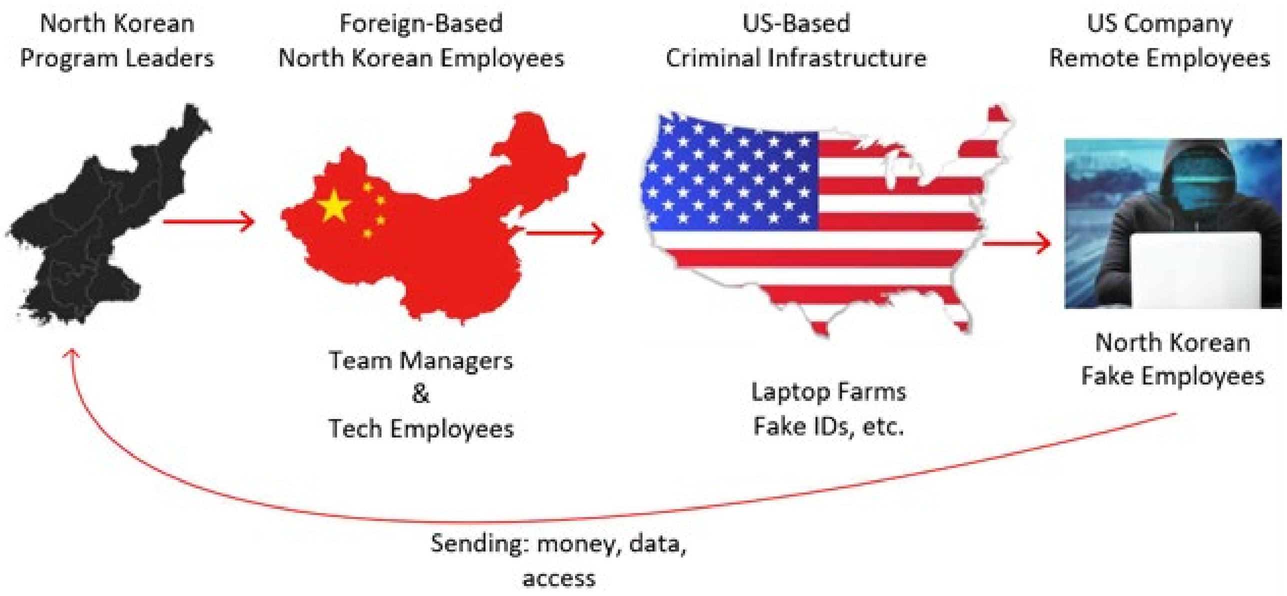
blackfog.com

© BlackFog Inc. 2024

Lessons Learned from KnowBe4

How a North Korean Fake IT Worker Tried to Infiltrate Us

“Within a few weeks, we heard from over a dozen other companies who either hired North Korean employees or had been besieged by a multitude of fake resumes and applications...”



North Korean Program Leaders

Foreign-Based North Korean Employees

US-Based Criminal Infrastructure

US Company Remote Employees

Team Managers & Tech Employees

Laptop Farms Fake IDs, etc.

North Korean Fake Employees

Sending: money, data, access

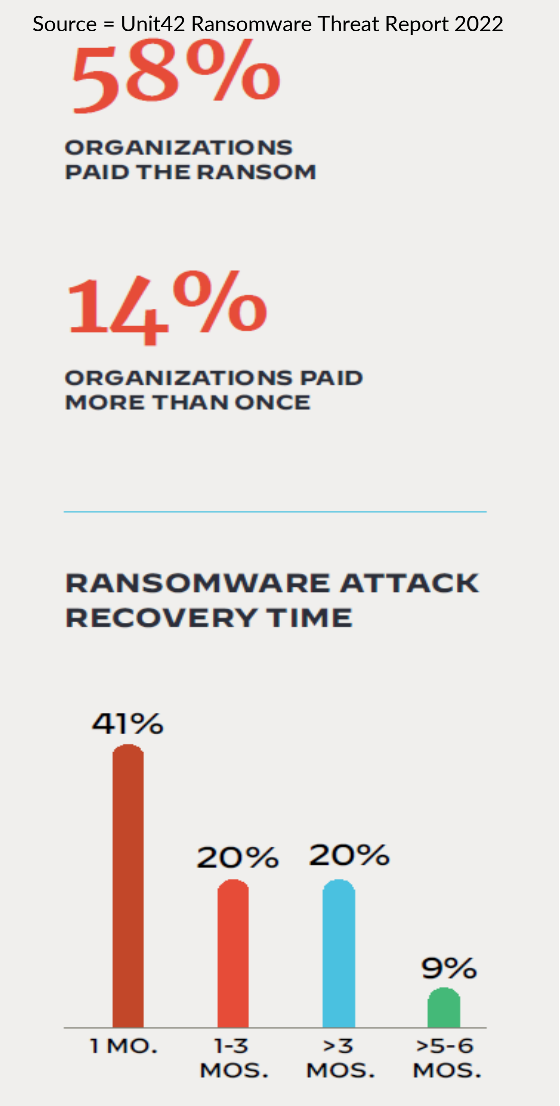
Ransomware trends

Attacks on cloud service providers

Ransomware writers are now targeting cloud service providers with network file encryption attacks as a way to hold hostage the maximum number of customers possible.

Intelligence gathering

Ransomware crime groups gather intelligence on intended victims, like studying SEC filings for an organization's financial position and use the information to scale ransom demands.



Source = Unit42 Ransomware Threat Report 2022

58% ORGANIZATIONS PAID THE RANSOM

14% ORGANIZATIONS PAID MORE THAN ONCE

RANSOMWARE ATTACK RECOVERY TIME

Casino Ransomware and Data Theft

Caesars

- Social engineering of IT vendor
- Likely paid $15M ransom

MGM

- Social engineering call to IT
- Cost expected to exceed $100M

BET SPORTS HERE
BETMGM
I'm having trouble communicating with the system. When the link is restored, your session will resume.
BET SPORTS HERE
BETMGM

Contract Security Requirements

Equipment Return

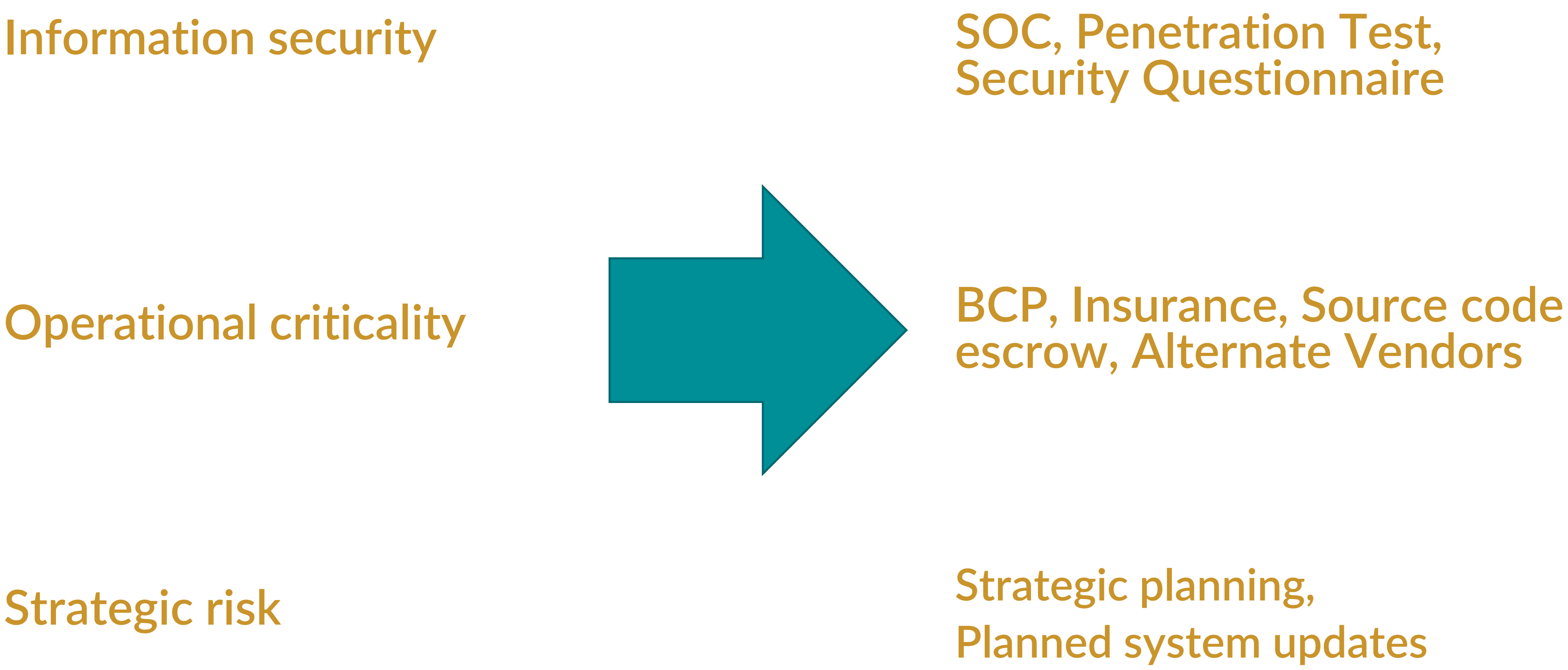
It is solely your responsibility to secure any sensitive data and permanently delete such data from the internal media storage prior to returning the equipment.

You shall hold _____ harmless from your failure to secure and permanently delete all such customer data.

> *"During the* ***term of this Agreement and for a period of one (1) year*** *thereafter, Consultant will not directly or indirectly disclose any such information, and will secure and protect such information…"*

How to Build a Vendor Management Program That Provides Value

Risk Assessment



Information security

Operational criticality

Strategic risk

SOC, Penetration Test, Security Questionnaire

BCP, Insurance, Source code escrow, Alternate Vendors

Strategic planning,
Planned system updates

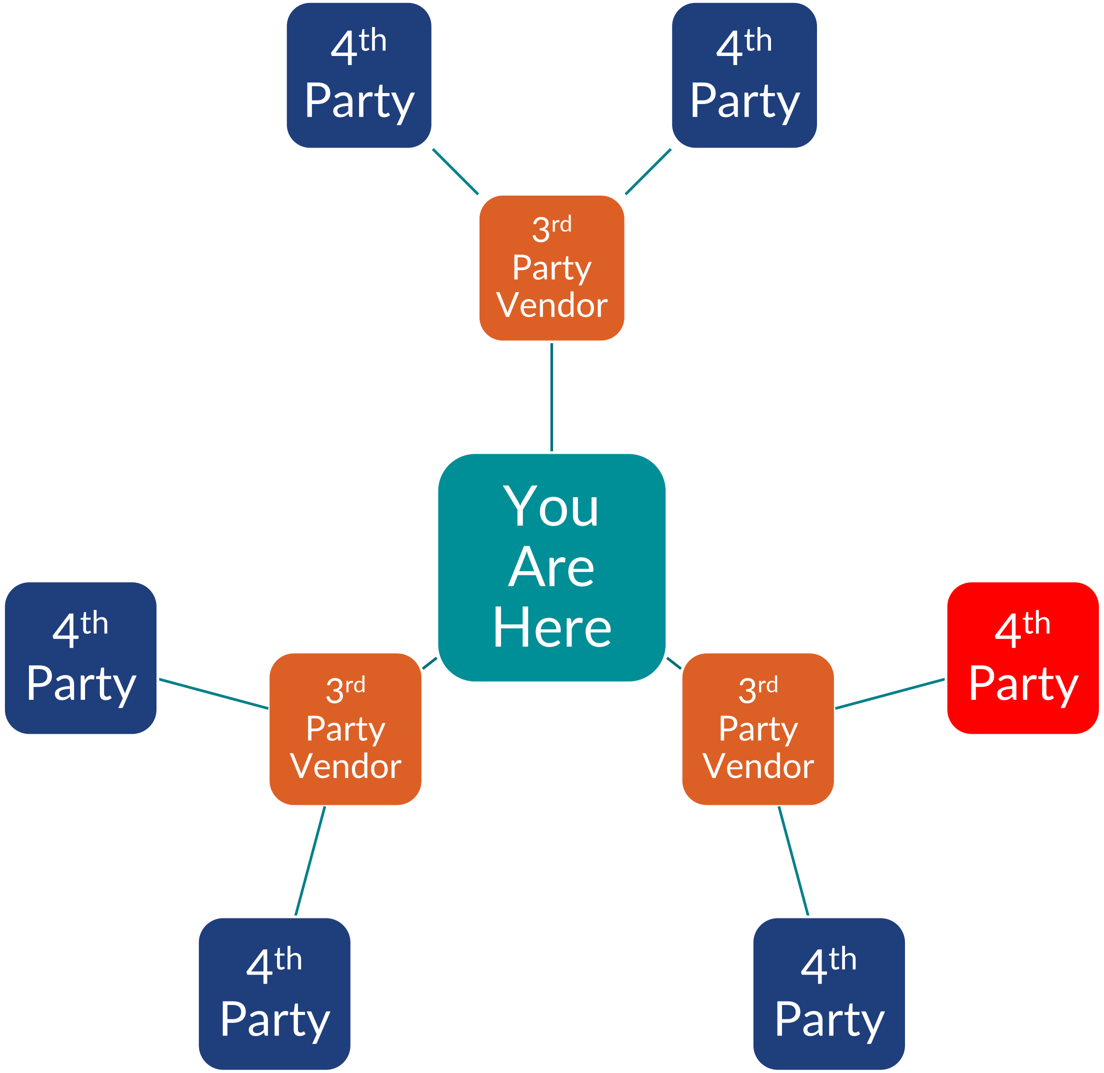
4th Party Security

Know your Vendors' Vendors – Contract, SOC Reports

Risk-Based Decisions

3rd Party Due Diligence Program

4th Party SOC Report

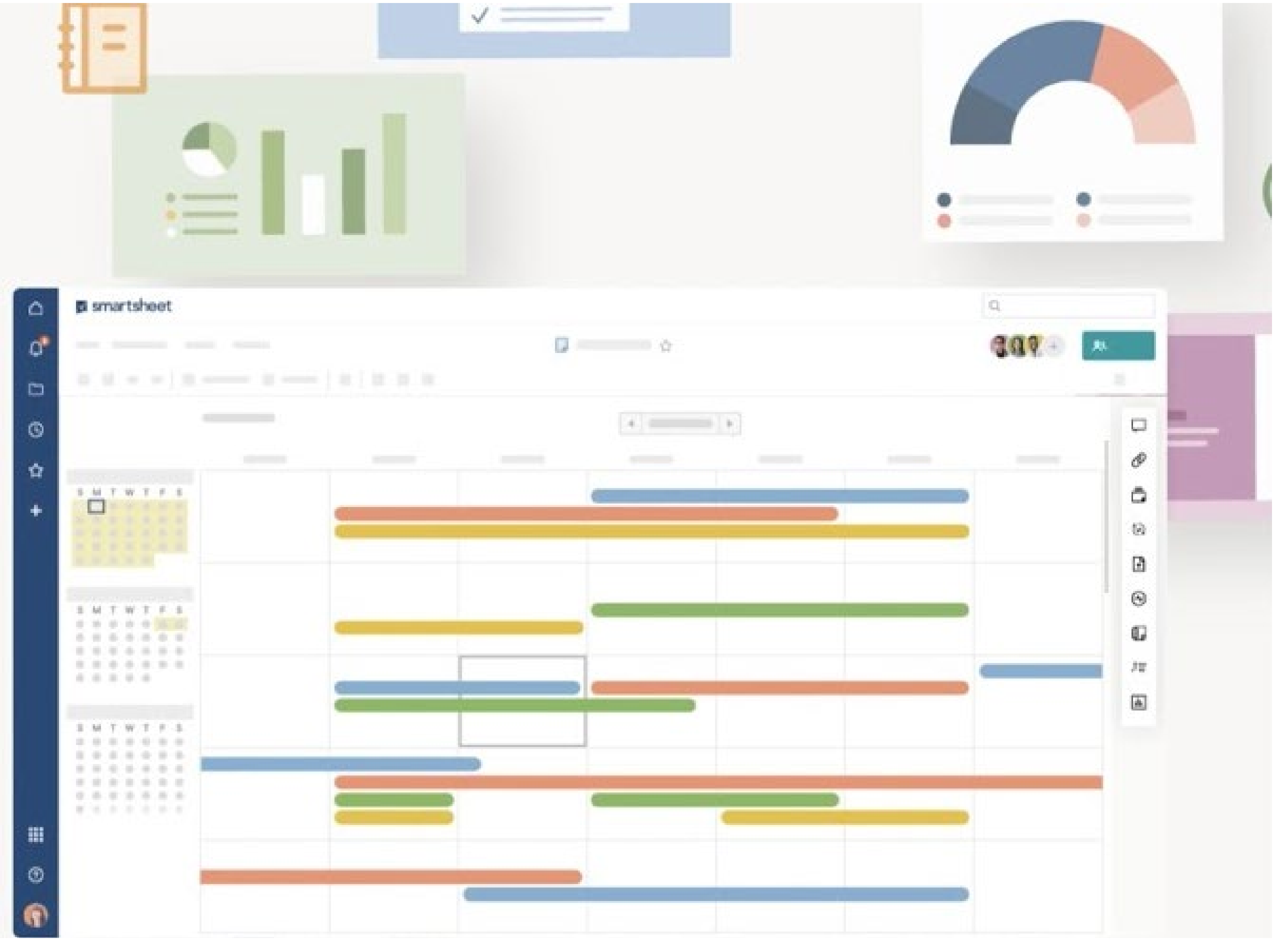


Initial and Ongoing Due Diligence

New Vendor Lead Time

Recurring Reviews - year-round

Team Responsibilities



Key Solution Benefits

Inventory

Risk Rating

Due Diligence Schedule and Storage

System Integration

NVENDOR

venminder

Tandem™

Solution Risks

Disconnected from Management's Processes

Outsourcing Task, not Responsibility

System & Organizational Controls (SOC) Reports

Type	What's in the report?	Who is the report for?
SOC 1	Internal controls over financial reporting and the related IT general controls	Intended audience is management, existing users (i.e., customers) of the system, and the user's financial auditors
SOC 2	Controls related to security, availability, processing integrity, confidentiality, and/or privacy	Intended audience is management and existing, prospective users of the system
SOC 2 +	Controls related to security, availability, processing integrity, confidentiality, and/or privacy plus additional subject matter such as HIPAA, HITRUST, CSA	Intended audience is management and existing, prospective users of the system
SOC 3	Controls related to security, availability, processing integrity, confidentiality, and/or privacy	For public use
SOC for Cybersecurity	Controls related to the cybersecurity risk management program	Perfect for management, board of directors, audit committee, investors, business partners, and other key stakeholders

Managing Third Party Risk through SOC Reports

SOC 1 – Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting

SOC 2 – Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

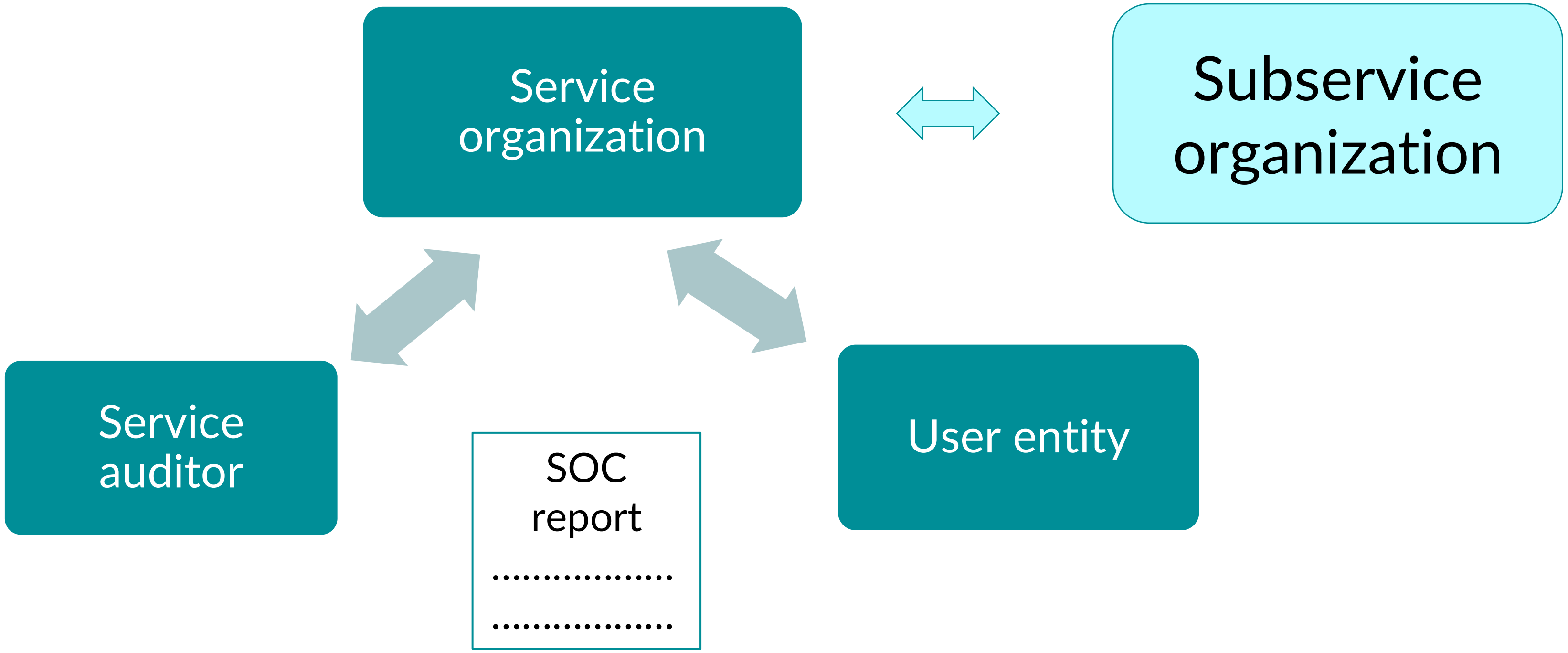
SOC 1 or 2 Report	Type 1	Type 2
Management’s description of the service organization’s system	As of a specified date	Throughout a specified period
The suitability of the design of the controls		
The operating effectiveness of controls	Not Applicable	

System & Organizational Controls (SOC)

Type 1

Type 2

Who's Who



Service organization

Subservice organization

Service auditor

SOC report

....

....

User entity

What’s in a SOC Report

Section 1 – Service Auditor’s Opinion

Section 2 – Management’s Assertion

Section 3 – Management’s Description of their System

Section 4 - Control Objectives, Controls, Tests of Operating Effectiveness and Results of Testing

What to Evaluate

- Examination Period
- Service Auditor
- Opinion
- Assertion
- Scope of Report
- Testing Procedures
- Findings/Exceptions
- Complementary User Entity Controls
- Any Subservice Organizations and their expected controls
- Anything else that you deem relevant to manage your risk

Some Important Definitions

Complementary user entity controls (CUECs)

- Controls assumed in the design of the service organization’s system to be implemented by user entities and are necessary to achieve the control objectives stated in management’s description of the service organization’s system.

Complementary subservice organization controls (CSOCs)

- Controls assumed in the design of the service organization’s system to be implemented by subservice organizations and are necessary to achieve the control objectives stated in management’s description of the service organization’s system.

System & Organizational Controls (SOC)

TRUE

OR

FALSE

What it is = An independent attestation of a service organization’s controls

What it’s not = Absolute assurance

Vendor Management Takeaways

Vendor Management Takeaways

1. Reconcile your vendor inventory

2. Include security requirements in contract reviews

3. Follow risk-based decisions –What matters to you?

4. Ensure SOC report address your concerns (Read it!)

5. Manage your vendor management solution

Questions?

Thank you!

Colin Taggart

Colin.Taggart@plantemoran.com
248-223-3235