EBOOK

AAFCPAs
great minds | great hearts

Best Practices for Reducing IT & Cyber Risks

AAFCPAs' Cyber & IT Security eBook

Introduction

Cyber threats are continuously evolving, with new structures and schemes emerging daily. This everchanging landscape of both cyber security and its infiltrators makes it difficult for individuals and corporations alike to know how to protect their Personal Identifiable Information (PII), client records, proprietary information, and other sensitive data. Examples of methods hackers use to perpetrate data breaches may include: malware, physical security breaches, third-party service providers, unsecured IT devices and Internet of Things (IoTs), malicious insiders, and social engineering.

In this ebook, AAFCPAs' IT Security professionals outline the most prevalent risks and share critical security measures to mitigate these risks, including those posed by:

- Social Engineering Attacks
- The Internet of Things (IoT)
- Software and Hardware Configuration Vulnerabilities
- Web Application Security Vulnerabilities
- Insufficient IT General Controls (ITGCs)
- Lack of Adequate Infrastructure/ Resiliency
- Outsourcing Services
- Physical Security Breaches
- Remote Workforces

AAFCPAs
great minds | great hearts

Table of Contents

Introduction
3

01
Social Engineering 4

02
Internet of Things (IoT) 8

03
Applications & Configurations 12

04
Web Applications 16

05
IT General Controls (ITGCs) 18

06
Outsourcing Services 23

07
Physical Environment 27

08
IT Infrastructure/Resiliency 31

09
Remote Workforces 35

Contact Us
38

About Us
39

01

Thwart Social Engineering Cyber Attacks

What is social engineering & what are the risks?

The human component of cyber security is the weakest link in protecting your organization against external threats. Recently, social engineering attacks have become the most prevalent type of threat within reported cyber breaches.

Social engineering is a malicious activity in which bad actors produce items such as false emails with the intent to persuade the recipient to unwittingly perform an action; for example, releasing sensitive information, and/or unknowingly planting malware on their network. Cyber criminals look for users who are naïve to social engineering attacks and/or those who are too busy to pay attention to warning signs.

Phishing

Phishing is the most common type of social engineering attack. It is often a poorly written email from an unusual sender. The goal is generally to get the recipient to click a link or download/view an attachment in order to provide authorization credentials (e.g. banking login), or even download and install a program that would monitor your keystrokes. This type of attack targets people with little to no cyber security awareness.

A common phishing example involves a Hacker simulating a notification that your password has expired. If the recipient falls for this they may provide the Hacker with access to confidential or proprietary information and also likely offer insight into how you derive your password pattern(s) (i.e. password1! often becomes password2!).

Spear Phishing

Spear Phishing takes the form of a highly convincing business email, which may appear to be sent from a legitimate business authority or an internal colleague. This form of phishing is not typically sent by random hackers. It is more advanced than regular phishing attempts because it targets individuals to gain financial, trade, or sensitive information.

For example, a hacker may impersonate a member of the finance department for one of your contractors. The hacker may send your Accounts Payable Clerk a “change of bank information” and provide new (fraudulent) account details. Once this is approved and processed by your AP Clerk or another employee, the next invoice from the real contractor will end up paid to the hacker’s account.

Whaling

Whaling schemes are sophisticated cyber phishing attacks directed specifically at senior executives and other high-level targets. The content of these messages is tailored for upper management, with the goal of tricking financial staff into making fraudulent wire transfers to bank accounts controlled by thieves. These targeted attacks are known to exploit the close relationship between CEO and CFO.

In the following real example, a hacker was able to gain access to the CFO’s Outlook account through use of the whaling technique. The hacker then

Related Insights:

Cyberattacks, Foreign Disinformation Campaigns Leverage Coronavirus Theme

researched email patterns, including who the CFO frequently emailed and for what purpose. This hacker also monitored the CFO's calendar for a strategic opening.

On the day of the incident, the CFO was out of the office with no access to email. The hacker waited patiently for this opportunity to send the AP Clerk a request via the CFO's email address for a large wire transfer to a specified bank account. The clerk checked with the company's Controller to confirm this odd request. The Controller was worried about delaying the CFO's request and executed the wire transfer to the hacker's account.

Many of the above-mentioned scenarios may be avoided by implementing the following countermeasures and prevention techniques.

What are Countermeasures/Prevention Techniques?

Maintain Security Awareness

Effective internal communications may help prevent damage from cyber-attacks. Organizations should establish employee security awareness campaigns to improve mindfulness of security threats.

- Continuously remind your employees to pay close attention and always be vigilant. Train them to be able to identify phishing emails. Provide regular examples of known phishing scams. Remind them that if something doesn't look right, it probably isn't.
- Outline your organization's "suspicious email response protocol," which should include a definition of technology controls, as well as a timely notification of your IT team to the phishing attempt and guidance on how to proceed.
- Remind your user community of the importance of internal control procedures, and your organization's zero tolerance policy on bypassing controls.

Establish Adequate Internal Controls… And Adhere to Them

Whaling attempts may appear as an email sent from a top executive requesting the recipient transfer money, for example. The message may appear urgent in nature and request that the recipient bypass the regular process in the interest of time and requestor's level of authority. This should always be a red flag.

Monitor & Test Your Controls

Organizations should test and evaluate the effectiveness of internal controls and their incident response procedures on an ongoing basis. A policy and/or procedure is good only if it is documented, challenged, known, and followed by all employees. In a potential incident, there is no time to respond to a broken process.

Test with Simulated Phishing Expeditions

AAFCPAs' Cyber and IT Security team assists clients with mitigating the risks of phishing, spear phishing, and whaling attacks by utilizing "white hat" social engineering methods. We gather information on clients, including their business structures, employees, and business dealings. We then collaborate with clients' IT and HR departments and perform phishing & whaling expeditions using e-mails or a web server to entice employees to provide information, click on a link, or open a file. We collect responses and report our findings to management on the risks uncovered.

Based on our findings, AAFCPAs advises clients on which employees need additional training, which helps our clients avoid future, real social engineering attacks that may cost them sensitive data breaches and stolen company funds.

Continuous Phishing Training

As part of an ongoing effort to reduce your risk of falling victim to social engineering scams, AAFCPAs advises clients to perform periodic phishing awareness training to continually remind employees about the potential of a phishing attack. The best approach is to perform simulated phishing campaigns in conjunction with employee phishing awareness training. Extend the reminder portion of the awareness with posters or infographics posted in the workplace.

Your best line of defense in protecting your organization against social engineering attacks is employee awareness. AAFCPAs advises clients to remain vigilant, assess your cyber security risks regularly, and maintain a cyber-aware community by educating users on the risks and consequences of social engineering attacks.

02

Secure Your Internet of Things (IoT)

What Is IoT & How Do Hackers Infiltrate Your Devices?

An increasing number of companies are installing IoT devices on their networks. IoT devices are typically "black box" devices, the inner workings of which are unknown to most users. For example, HVAC systems, smart fridges, computer printers, and even cars can contain IoT-enabled technology that connects through WiFi or cellular and therefore can be considered IoT devices.

With PCs, there are many different types and manufacturers, but most of them run via Windows, MacOS, or Linux. In contrast, there are about as many unique operating systems for IoT devices as there are manufacturers. It is currently estimated that approximately 2 million IoT devices are vulnerable to complete takeover, according to Threatpost. Hackers can discover vulnerabilities of these devices or their manufacturers through documents published on the internet or by monitoring communication to and from your IoT devices.

Which Common Devices Are At Risk?

HVAC Systems

HVAC systems often reside on the company's internal network and can be capable of remote and internet connections. This device is not secured, which means an outsider may be able to breach the HVAC system. While it is only a heating and cooling mechanism, the innocence of the breach is deceptive. Hackers can use this device to obtain access to other parts of an organization's network.

For example, in the Target data breach of 2013, it is suspected that hackers stole credentials from the retail chain's HVAC company in order to access the network. Hackers then used this network access to steal customer credit card data. According to USA Today, this breach affected 41 million customer accounts and forced Target to pay $18.5 million in restitution.

Multi-Function Copier (MFC) Devices

MFC devices, such as computer printers, are vulnerable. Once a hacker gains access, they can view items that have already been printed and receive unlimited access to future print items.

Some companies have taken extra precautions to protect print jobs, including providing each employee with an individual PIN number in order to start their print/copy job. While this strategy does help to reduce the number of printed pages left on the printer for an extended period of time, hackers can still use brute force methods to gain access. This brute force approach relies mainly on automated programs that are able to enter a large quantity of combinations at once in order to find the desired PIN.

Hackers can further infiltrate the MFC devices if they possess internet access. Using the device's internet capabilities, they can send employees' print jobs to other locations. These locations could include other computer printers, or other virtual file folders.

Related Insights:

COVID-19 has challenged businesses to think about operations in a new way. AAFCPAs advises clients to assess and advise employees of risks associated with home Internet of Things (IoT) devices. Read how to Overcome Cyber Security Challenges of a Remote Workforce on p.35.

What Are Countermeasures/Prevention Techniques?

AAFCPAs advises clients to understand the connections and data that their IoT devices generate, and to ensure security is regularly assessed and tested.

Vulnerability Scan

IoT devices are black box systems, and companies must identify and understand security risks in order to determine appropriate countermeasures. AAFCPAs conducts vulnerability scans for clients to identify, examine, and classify their IoT devices, connections, configurations, and monitor the types of data transmitted.

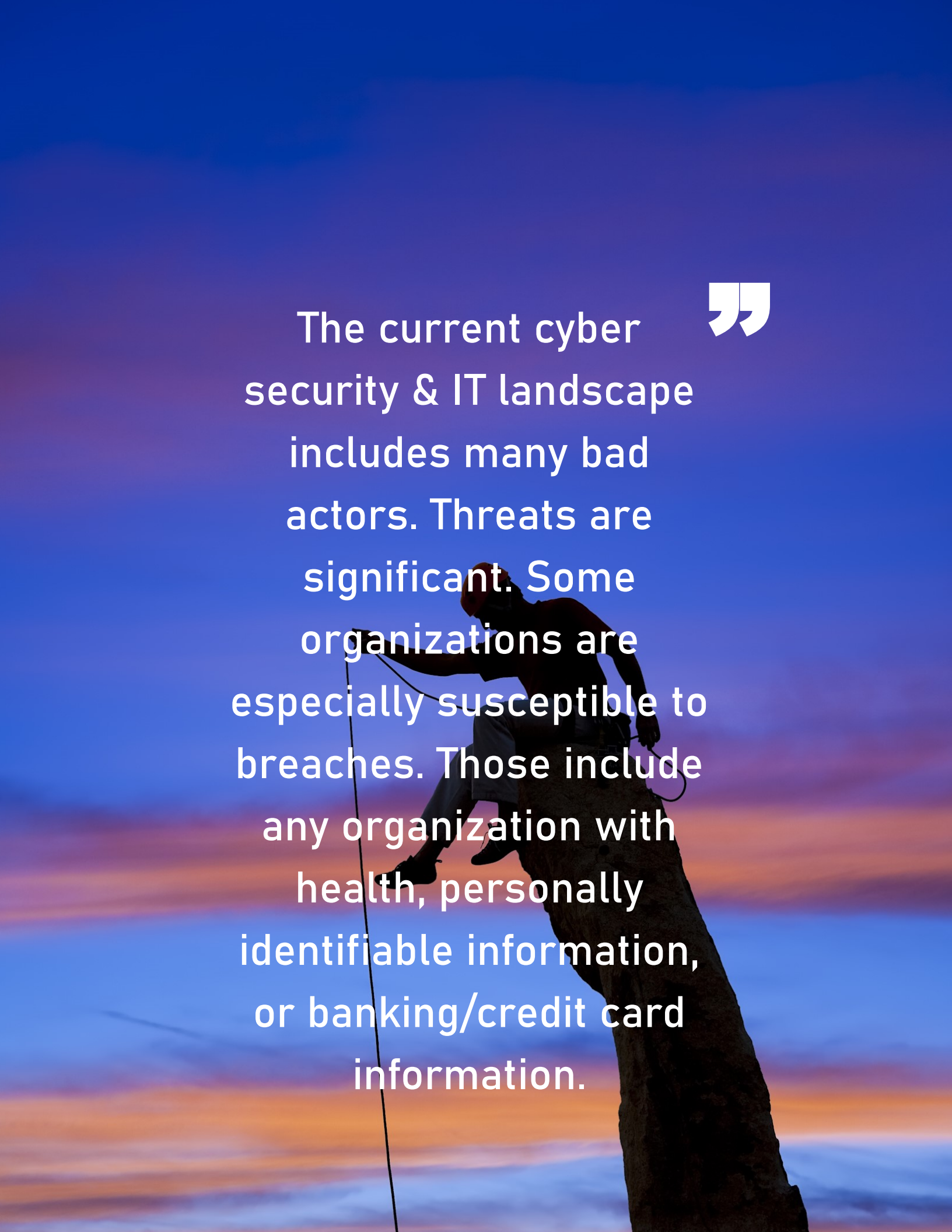
Your best line of defense in protecting your organization's IoT devices from hackers is identifying all of the devices that reside on your organization's network and understanding their vulnerabilities.

The results of the vulnerability assessments are analyzed by AAFCPAs' cyber security team to advise on necessary steps to protect your organization, secure the IoT devices from potential hacker exploits, and keep your sensitive data safe. AAFCPAs recommends that organizations conduct a vulnerability scan on a quarterly basis and each time a new type of device is added to the network, as this constitutes an infrastructure change.

Network Inventory

IT staff should be aware of all devices on the network in order to understand their capabilities and determine any potential updates for those devices. AAFCPAs advises clients to conduct an inventory of all devices currently on your network.

When new devices are introduced to the network, your organization should review applicable IT policies and procedures, such as the written information security policy (WISP). For example, if a new camera is added to your network, your IT staff must confirm if the physical security policy is still applicable. If your organization's WISP requires antivirus protection to be installed on all devices on your network, but these new cameras are not capable of having endpoint protection installed, then you would need to identify compensating or mitigating controls so the new devices do not create unnecessary risks for the company.



The current cyber security & IT landscape includes many bad actors. Threats are significant. Some organizations are especially susceptible to breaches. Those include any organization with health, personally identifiable information, or banking/credit card information.

03

Manage Vulnerabilities in Your Applications & Configurations

Despite the best efforts of IT teams, organizations continue to be plagued with security vulnerabilities in their systems by both internal and external threats.

The most common vulnerabilities are poor configurations and outdated/ unpatched systems or applications. These vulnerabilities may expose your organization to the risk of hackers gaining access to sensitive employee or client data.

What are Countermeasures/Prevention Techniques?

Change Management

AAFCPAs advises clients to establish and document their process for reviewing and implementing changes to the IT environment. Change management is a comprehensive system which monitors the additions, adjustments, and decommissions of any applications or infrastructure for the organization.

Any new items, modifications, or deletions require this clear tracking system to streamline their integration into or out of the existing system. Change management systems can also track what approvals are required, the collection of necessary sign offs, and manage requests for proposals.

AAFCPAs assists clients in developing, enhancing, and/or implementing change management processes.

Internal systems historically have more vulnerabilities, often due to either inconsistent configurations or the mindset that once the external is secure no one will be able to breach the internal.

Implement Secure Configurations

The most prevalent security weaknesses exploited by hackers include system, server, and application configurations. These configurations are often poorly protected, as the default settings allow hackers to easily obtain sensitive data.

Companies should adopt a standard for secure configurations, such as NIST, SANS, or CIS. Each of these frameworks maintain standards for configuring operating systems and developing a baseline for security configuration. The adoption of a uniform set of standards will help to create a consistent configuration for the deployment of new or modified systems.

AAFCPAs conducts configuration reviews for best practices or in order to ensure clients comply with existing, adopted standards.

Protect Both Outside and Inside the Firewall

It is imperative that organizations secure both internal and external systems or applications. When someone exploits an external system or application, in most cases, they will then use that system to gain access to internal systems. Internal systems historically have more vulnerabilities, often due to inconsistent configurations or the mindset that once the external is secure, no one will be able to breach the internal.

It is possible to breach an internal system without accessing the external system first. For example, internal breaches may be achieved by a former employee who still has access to the system, or by family/friends of remote employees who use the virtual private network (VPN) to work from home.

Organizations can prevent these exploitations of their system by implementing the above change management directives and secure configuration standards. In addition, management must be vigilant to ensure the processes are followed for all changes, so that anomalies like former or remote employees do not result in gaps for an organization's security.

AAFCPAs supports clients' efforts by conducting firewall configuration reviews or assisting in implementation and design of firewalls and demilitarized zones.

Vulnerability Scans

Vulnerability scans inspect potential points of exploitation on a computer or network based on known vulnerabilities. These scans allow organizations to locate and classify gaps in security and improve protection through remediation.

For example, AAFCPAs' IT security specialists conduct IP and port scans to determine which services and applications are currently running. These scans identify which parts of the system/application are vulnerable and require reinforcement, such as a firewall configuration change, new firewall rule, web server patches, an additional system for protection, or an update to an application.

Penetration Tests

A penetration test is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities. Penetration tests can confirm the results of a vulnerability scan and assert false positives with certainty. Penetration tests should follow vulnerability scans, as they use the knowledge from the scan to understand which weak points should be further tested for security purposes.

AAFCPAs' penetration tests attempt to exploit any noted vulnerabilities through a "red team" and "blue team" approach. The designated red team will attempt to exploit the specified vulnerability, while the blue team attempts to defend against these calculated attacks. These teams are determined ahead of time and may consist of an individual or a group, such as AAFCPAs' cybersecurity team (red) versus a client's internal IT team (blue). The purpose of the competition between these teams is to test the vulnerabilities and defenses of a system or application within an organized setting.

It is possible to breach an internal system without accessing the external system first.

For example, the Apache web server application regularly receives patches and updates from Apache to mitigate security flaws. When a vulnerability scan suggests that a necessary patch is missing in the client's version, the designated red team may be deployed in a penetration test to exploit the potentially vulnerable web server while the blue team attempts to block their intrusions.

AAFCPAs advises clients to annually assess internal and external vulnerabilities through scanning and testing their systems. However, this should be increased to a quarterly assessment when a new system has been added or a configuration has changed.

04

Fortify Your Web Applications

Custom web-based business applications are increasingly attractive because they allow companies to improve employee and customer user experiences with enhanced flexibility and efficiency. Some custom business app platforms tout that "creating your own custom apps is easy, even if your programming knowledge is non-existent." However, this ease and accessibility may lead to unanticipated security vulnerabilities.

According to Imperva, in 2019 web application and database vulnerabilities increased by 17.6% from 2018 and 44.5% from 2017. Imperva also notes that "almost half of the vulnerabilities (47%) have a public exploit available to hackers." Hackers can use these exploits to enter your organization's network and access your systems.

What Are Countermeasures/Prevention Techniques?

In most situations, configuration or programming errors are the leading cause for web application vulnerabilities. These errors may be identified by performing a web application scan and/or code reviews.

Web Application Vulnerability Assessment

AAFCPAs advises clients to conduct regular web application vulnerability assessments when they have systems exposed to the internet. Exposure is of particular concern when sensitive data resides on the internet or if applications are developed and managed internally.

AAFCPAs' web application vulnerability assessments identify vulnerabilities such as HTML or SQL injections, cross-site scripting (XSS), and URL redirections. When these vulnerabilities are present, hackers could modify the code or links in your web applications.

Vulnerabilities are likely a result of breakdowns in your organization's processes.

Evaluate Processes

While it is important to remediate issues shown in scan results, AAFCPAs' cyber security experts advise clients to examine root causes and enhance internal processes to reduce or eliminate the reoccurrence of such findings.

Vulnerabilities are likely a result of breakdowns in your organization's processes. AAFCPAs evaluates clients' existing processes related to change management and Software Development Life Cycle (SDLC) and provides guidance to improve security measures moving forward.

Regularly Assess the Most Prominent Security Risks

The Open Web Application Security Project (OWASP) is a global nonprofit community that identifies and provides guidance on the most prominent vulnerabilities in web-based applications. The OWASP Top 10 List of Risks represents a broad consensus about the most critical security risks to web applications and is considered the ideal starting point for web application security.

AAFCPAs encourages clients—especially those who created or customized web-based application(s)—to adopt the OWASP awareness document within their organization. AAFCPAs completes OWASP analysis for clients to improve the security and quality of their code. OWASP scans go beyond those of a Web Application Scan to include source code reviews.

05

Optimize Your IT General Controls

Information Technology General Controls (ITGCs) help organizations guard their systems and operations against IT-related risks in critical business areas like finance, purchasing, and payroll. ITGCs are the foundation for the overall IT control environment as they provide the assurance that systems operate as intended and that output is reliable. (For public companies, these controls support financial auditing, as they collectively uphold Sarbanes-Oxley (SOX) compliance requirements.)

AAFCPAs Groups ITGCs Into Five Main Categories:

ITGCs can be grouped into five major categories: Access to Programs and Data, Change Management, Program Development, IT Operations, and Network and Systems Security.

1. Access to Programs and Data

AAFCPAs provides guidance to clients related to risks associated with system access. Only the most appropriate and authorized users should have permissions to access applications and sensitive data. Further, these users should be made aware of their responsibilities to maintain the security of these applications and sensitive data.

To address these risks, AAFCPAs assesses controls related to five objectives:

i. We determine if information security is managed to guide consistent implementation of security practices and that users are aware of the organization's position with regard to information security, as it pertains to financial or sensitive data.

ii. We determine if logical access to applications and data is appropriately restricted by the implementation of identification, authentication, and authorization mechanisms to reduce the risk of unauthorized/inappropriate access to the organization's relevant systems.

iii. We determine if procedures have been established so user accounts are added, modified, and deleted in a timely manner to reduce the risk of unauthorized/inappropriate access to the organization's relevant financial reporting or sensitive data.

iv. We determine if effective controls are in place to monitor the maintenance of access rights to the organization's relevant financial applications or sensitive data.

v. We determine if controls are used to provide appropriate segregation of duties within key processes and that they are followed.

> *AAFCPAs advises clients to implement a least permissive, and resource-appropriate approach related to programs and data access for employees based on best practices and mandated regulations.*

2. Program Changes

AAFCPAs provides guidance to clients on identifying and addressing risks related to program changes, including that they are authorized, tested and approved, and are restricted to being performed by properly authorized and appropriate staff who are independent from those that developed the changes.

To address these risks, AAFCPAs assesses controls related to three objectives:

i. We determine if controls are in place to ensure that any changes to the systems/applications providing control over financial reporting or sensitive data have been properly authorized by an appropriate level of management.

ii. We determine if controls are in place to ensure that changes to applications and systems used during the financial reporting process—or which process or store sensitive data—are tested, validated, and approved prior to being placed into production.

iii. We determine if controls are in place to restrict access for migrating changes into the production environment for systems and applications used during the financial reporting process—or which process or store sensitive data.

3. Program Development

AAFCPAs provides guidance to clients on addressing risks related to program development initiatives to ensure they are authorized, tested and approved, and that migrated data has maintained its integrity.

To address these risks, AAFCPAs assesses controls related to four objectives:

i. We determine if management has controls in place to ensure that new program and infrastructure development projects and acquisitions have been approved by an appropriate level of both IT and business management.

ii. We determine if management has controls in place to ensure that an adequate program development methodology is in place and is followed for the development or acquisition of systems/applications used during the financial reporting process.

iii. We determine if management has controls in place to ensure there is adequate testing for the development or acquisition of systems/applications used during the financial reporting process and that testing is signed off by both of the users at an appropriate level of IT and business management.

iv. We determine if management has controls in place to ensure that data migrated to the new application or system used during the financial reporting process retains its integrity.

4. Computer Operations

AAFCPAs provides guidance to clients related to risks associated with computer operations. This includes ensuring that batch jobs are controlled, data is available when needed, and end user computing such as excel or report writing tools are governed by the same level of IT General Controls that the application uses.

To address these risks, AAFCPAs assesses controls related to five objectives:

i. We determine if management has implemented procedures to ensure accuracy, completeness, and timely processing of system jobs, including batch jobs and interfaces, for relevant financial reporting applications or data.

ii. We determine if management has implemented appropriate backup and recovery procedures so that data, transactions, and programs that are necessary for financial reporting can be recovered.

iii. We determine if effective procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media relevant to systems and applications used during the financial reporting process.

iv. We determine if appropriate controls are in place over the backup media for systems and applications used during the financial reporting process. This includes ensuring that only authorized people have access to the tapes and tape-storage or to electronic storage systems containing backups.

v. We determine if management has implemented appropriate policies and procedures to ensure ITGCs are properly applied to the end-user computing environment.

5. Network Security

AAFCPAs provides guidance to clients to ensure IT systems are not vulnerable to attack or penetration.

To address these risks, AAFCPAs determines if management has implemented safeguards to prevent access to systems and data by unauthorized parties. Such safeguards could include firewalls and firewall patch management, network segmentation, intrusion prevention and detection, minimum requirements to connect to the network, vulnerability assessments or penetration tests, wireless encryption method, and network monitoring.

Your best line of defense in protecting your organization from risks associated with the failure of ITGCs (and failure of a SOX audit) is to annually test the design, implementation, and operating effectiveness of your controls.

AAFCPAs evaluates clients' ITGCs in order to provide assurance over the security, confidentiality, processing integrity, and availability of data. Our evaluations identify, and where needed, document each control, test the design, and where desired, assess operating effectiveness. AAFCPAs provides management reporting related to all findings, risks associated, and recommendations to improve and implement changes.

06

Mitigate Risks Associated With Outsourcing Services

If you outsource services such as payroll processing, loan servicing, data center/co-location/IT Managed Services, Software as a Service (SaaS), or medical claims processing, you rely on the service provider to keep your data secure, maintain confidentiality, integrity of processing, availability of services or systems, and/or privacy. However, AAFCPAs reminds clients that outsourcing may expose your organization to risk and underscores the need for effective vendor due diligence.

The American Institute of Certified Public Accountants states “Management of a user entity is responsible for assessing and addressing risks faced by the user entity related to financial reporting, compliance with laws and regulations, and the efficiency and effectiveness of operations. When a user entity engages a service organization to perform key processes or functions, the entity exposes itself to additional risks related to the service organization’s system. Although

management of a user entity can delegate tasks or functions to a service organization, the responsibility for the service provided to customers of the user entity cannot be delegated. Management of the user entity is usually held responsible by those charged with governance (for example, the board of directors); customers; shareholders; regulators; and other affected parties for establishing effective internal control over outsourced functions."

A service organization is part of your financial system of controls if they affect any of the following:

- The classes of transactions in your operations that are significant to your financial statements;
- The procedures, both automated and manual, by which your transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements;
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in your financial statements involved in initiating, recording, processing, and reporting your transactions;
- How your information system captures other events or conditions that are significant to your financial statements; or
- The financial reporting process used to prepare your financial statements, including significant accounting estimates and disclosures.

How Do You Know If Your 3rd Party Service Provider Has Adequate Controls?

Systems and Organization Controls (SOC) reports provide user organization management with the information they need related to the service organization's controls to help assess and address the risks associated with an outsourced service.

SOC 1: Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting

The SOC 1 report is designed to address internal controls over financial reporting and concentrates on a service organization's controls as they relate to the processing of your transactions. For example, a payroll processing company receives your records and banking instructions for all employees. This work is outsourced to the payroll company, but you are still responsible for the work and how it impacts your financial statements. If the payroll company cannot demonstrate they have adequate and suitably designed controls that operate effectively, they are viewed as a greater risk to clients and as a result are less likely to be hired for these outsourced services.

AAFCPAs advises our clients to request a SOC 1 from their service providers when the outsourced services have a relationship to their financial reporting. The SOC report should be assessed by the user organization and controls specified in the User Organization Controls section should be evaluated for whether they should be implemented at the user organization. Other SOC reports, such as those for subservice providers, should also be requested because the service provider may be relying on the services and controls of the subservice provider.

SOC 2: Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

The SOC 2 report addresses a service organization's controls for operations related to the security, confidentiality, processing integrity, availability, and privacy of IT, personally identifiable information (PII), and other sensitive information for their clients. For example, an organization that prints and/or mails statements for hospitals or other medical institutions may require a SOC 2 report. Hospitals often outsource the printing and mailing of client statements to an external vendor. The hired organization receives extensive confidential information, including names, addresses, diagnoses, and medications for patients. A SOC 2 report will provide reasonable assurance that information is securely received and transmitted for the service organization's clients.

AAFCPAs advises our clients to request a SOC 2 from their service providers when the outsourced services have a relationship to their financial reporting. The SOC report should be assessed by the user organization and controls specified in the User Organization Controls section should be evaluated for whether they should be implemented at the user organization. Again, SOC reports for subservice providers should also be requested.

Vendor Risk Management Program

AAFCPAs advises clients to develop, document, and adhere to a vendor risk assessment program, which should include requirements for SOC reports and other attestations. Organizations are urged to only outsource services to a vendor that meets compliance standards.

The controls tested during a SOC 1 report will determine whether the service organization has sufficient internal controls over processes that can impact your company's financial reporting. Similarly, SOC 2 examinations will test the controls that protect the systems or data of which service organizations have access.

When outsourcing the processing of financials or large amounts of sensitive data, you need to trust that the service organization has the systems and controls in place and in working order to protect your information.

07

Secure Your Physical Environment

Data and IT Security goes well beyond cyberspace. The security of your physical office space may also be at risk. A successful physical breach by an outsider could produce unauthorized access to packages, equipment, documents, as well as threats of theft and employee safety.

Piggybacking

Piggybacking, or the close following of an employee through company entrances, is a risk to physical office spaces during business hours. Employees often allow visitors to roam the space without supervision, assuming they are a new employee or there for another approved purpose, such as building maintenance.

Once intruders gain discrete access to your office, they could steal equipment or install devices on your network, which would then allow them to access your systems remotely.

In order to reduce the risk of piggybacking, an organization should reinforce strict physical controls. Some best practices include visitor sign-in, providing visitors with a temporary badge and accompanying visitors at all times. Office entry doors should be locked at all times except the front door if there is a receptionist present. Employees should be aware of surroundings and alerted/ cognizant when opening restricted area doors in case they have been followed, making sure the door behind them is closed and no one piggybacks.

RFID Badge Cloning

Employees should always keep their badges with them, and should shield them when in small spaces, such as elevators. Shielding will make it more difficult for intruders to clone badges. RFID badge cloning can be achieved from anywhere between a few inches to several feet away. Badges may be shielded using RFID blocking wallets or aluminum foil, but these will only shield some badges. For more comprehensive protection, AAFCPAs recommends the use of radio frequency shielding bags, which block cell signals, Wi-Fi, satellite, and Bluetooth frequencies.

Parking Lots

AAFCPAs advises clients to evaluate risks posed by view obstructions, such as overgrown shrubs or poor exterior lighting.

Building Entrances

Clients are urged to ensure that all doors and windows have working locks that are always secured outside of business hours—and during business hours if

they provide access to restricted areas. This includes securing windows above the ground floor, which may be breached by someone with a ladder, a tree, or other means of elevation.

AAFCPAs advises clients to assess which areas are secure. For example, the doors to the reception area or conference rooms may not require badge access or other security measures. These areas are not secured from intruders.

What Are Additional Countermeasures/Prevention Techniques?

Physical Security Assessment

AAFCPAs' IT & cyber security team can assess the physical security of your organization based on common, potential external and internal vulnerabilities. Once the assessment is complete, the team will provide photos and other documentation with clear suggestions for improvement on the inside and outside of the building. Physical breach attempts are part of the physical security assessment. These attempts will be made by incognito members of AAFCPAs' security team.

In addition to assessing vulnerable points of entry, the attempted breach will put your organization's existing security measures and employee awareness to the test. Strategies used to gain physical access may include: piggybacking or shuffling in discretely behind an authorized employee; cloning employee badges; and breaching secondary (e.g. service) entrances without being observed.

If a physical breach is successful, our security experts will then further evaluate the availability of sensitive data and the trust levels of employees. This may include searching for: unattended and unlocked computers; monitors in public areas with sensitive information displayed; physical network jacks left unprotected; and/or documents left in a printer, on/in desks, or in unsecured employee mailboxes.

Employee Education and Vigilance

Regardless of the many safety measures in place, employees may still allow for cracks in your physical security shield. AAFCPAs recommends clients conduct annual employee education programs to ensure your team remains vigilant. Some best practices include:

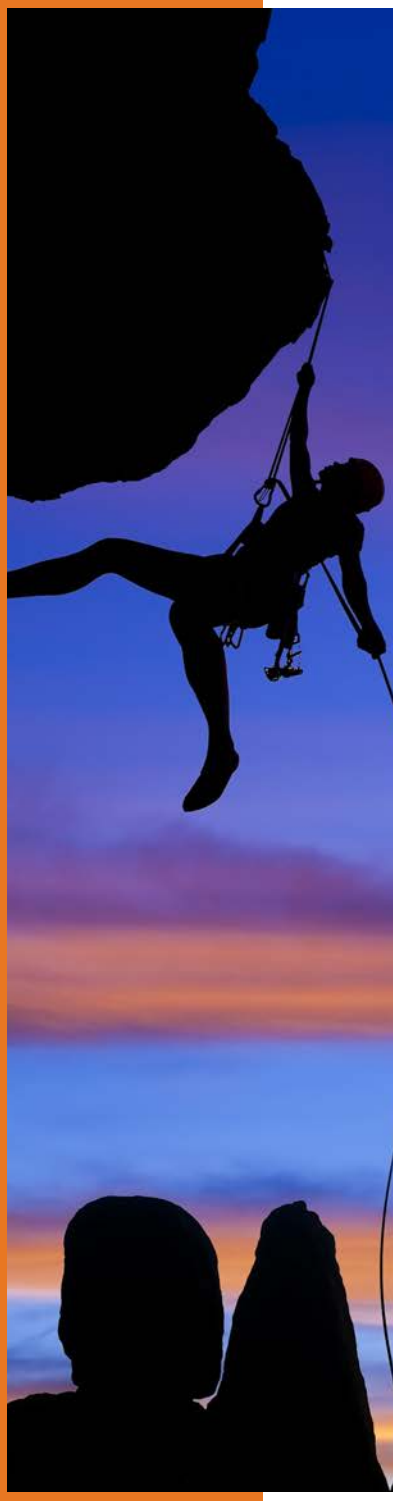
- **Clean Desk Policy** – Employees should remain vigilant about what is accessible/visible on their desk, such as client information, account passwords, or other sensitive data.
- **Locked Workstations** – Employees should be expected and reminded to lock their computers/workstations when they leave their desks.
- **See Something, Say Something** – Employee should be encouraged to greet all unfamiliar faces and offer assistance, as well as ask why they are there. This gives employees an opportunity to introduce themselves to a colleague they may not have met. As an additional precaution, AAFCPAs suggests that management implement photo IDs for employees and badges for all visitors.

08

Secure Your IT Infrastructure & Create Resiliency

IT infrastructure is the combination of hardware, software, communications, data centers/hosting services, and human resources that allows an organization to deliver information technology services to its constituent communities.

IT resiliency refers to an organization's ability to avoid or minimize business disruption when the IT infrastructure is challenged by planned or unplanned events, such as the novel Coronavirus. IT resiliency is at the core of an effective IT strategy, designed to ensure organizations can quickly get back to business after something goes wrong, as well as how to protect your organization from threats in the first place.



Planned or unplanned events that could impede your ability to deliver optimal services may include: production and/or migration failure of systems and/or applications, turnover among key IT staff, man-made and natural disasters, cyberattacks, and malicious activities by known or unknown parties. Any of these events may disrupt or even paralyze an enterprise if proper planning and controls are not in place.

What Are Measures to Improve IT Infrastructure Resiliency?

Document and Test Your Business Continuity Plan

Business Continuity Plans (BCPs) are essential to successfully conduct business seamlessly when disruption strikes. Having a working BCP in place in advance of a disruptive event helps to lessen the impact on people, processes, and systems.

AAFCPAs' Business & IT Consulting practice advises clients to first answer the questions: "What do we need most?", "How long can we be without?", and "How much data can we afford to lose?" The answers to these questions generate a Recovery Time Objective (RTO) and Recovery Point Objective (RPO). From there, a specific plan to address the needs of each service may be developed.

Document and Test Your IT Disaster Recovery Plan

An IT Disaster Recovery Plan (DRP) is a documented and tested process or set of procedures which ensures your organization can recover IT systems, services, and data following an event. DRPs should be tailored to your business size, industry, and specific IT infrastructure. The plan will be multi-discipline and include other departments outside of IT. A risk-based approach will drive answers to "How will we work?", "Where will we work?", "What is the impact to the business and our constituents?", and "Who will communicate to our constituents?" Once crafted, periodic testing of the DRP should be executed as part of your BCP in order to support business operations.

Sound Backup and Recovery Strategy

Organizations must implement strategies that protect both their data and their ability to access it. These strategies are only a single component of a comprehensive BCP and broader DRP.

The Backup and Recovery Strategy should include routinely scheduled backups of your business' critical systems. Routine is subjective and driven by RTO and RPO requirements specific to the environment being backed up and recovered.

Robust Risk Assessment

Understanding where risks exist in your technology enterprise is paramount to your ability to effectively manage them. Risks come in many forms and are as individual as your organization. Risks exist in aged technology; outdated solutions; access control deficiencies of incoming; existing and departed staff; inappropriately configured systems; poor password management practices; and a lack of employee training and awareness, to name but a few.

AAFCPAs advises clients to perform regular top down risk assessments as a solution to help identify, prioritize, and remediate deficiencies.

How Can AAFCPAs Help?

AAFCPAs recommends performing an IT Risks and Controls assessment first. Once completed, visibility to high risk concerns will be unveiled and then may be addressed. If cyber security is of strong concern, network penetration and cyber assessments may also be employed. If you host private and/or confidential information covered by HIPPA, GDPR, PCI, or other local, state, federal, or international governing requirements, these services should be considered.

AAFCPAs' Business & IT Consulting practice advises clients on improving their IT Resiliency with recommendations that are right-sized and tailored to be appropriate given each client's resources and specific IT infrastructure requirements.


Threats can be mitigated.
For every risk and threat,
there is a mitigating
action.

09

Overcome Cyber Security Challenges of a Remote Workforce

COVID-19 has challenged businesses to think about operations in a new way, and in many cases, your IT specialists may be supporting employees for the first time ever that were never intended or conceived to be remote or fully remote.

With an increased risk of employees falling prey to cyber-attacks, AAFCPAs advises clients to create new policies and leverage technologies to keep their company's data and employees safe while working in their remote and often home environments. Our IT Security Specialists have provided the following key considerations and best practice recommendations to ensure clients can support a remote workforce while maintaining secure network access.

Cyber Security Questions to Consider

- Do you have a set of standard, practicable measures to ensure IT security of a remote workforce?
- Do you provide devices to your employees or do you allow a bring your own device (BYOD) security scheme?
- Have you informed and educated your workforce about the additional dangers during this time?

What Countermeasures/Risk Mitigation Techniques Can I Implement?

Ensure Logical Security of Devices at Home

Whether your users are working on company-issued computers or BYODs, the following tips can help secure at home use:

- Ensure users have changed the default name of their home Wi-Fi and confirm network passwords are unique, strong, and changed. Additionally, advise users to turn on their wireless router's maximum encryption setting (any router with encryption settings below WPA2 should be replaced with one that is more capable), and disable SSID broadcasting to the general public. Ensure the wireless router's firewall is turned on/or install a good firewall solution.
- Ensure user devices have up-to-date operating systems, security software, and firewalls. Tools can be used to verify the most up to date patches have been applied.
- Use a virtual private network (VPN) or remote desktop protocol (RDP) to access your network.
- Assess and advise employees of risks associated with home Internet of Things (IoT) devices, such as smart TVs, speakers, sprinklers, thermostats, video doorbells, printers, and more… These devices should not be on the same network used to access company data, but rather on a secondary or guest network.

Ensure Physical Security of Devices at Home

Bad actors, hackers, and thieves rely to a great extent on weaknesses in users. AAFCPAs advises clients to consider the following weaknesses to ensure your employees' devices are physically secure:

- Discourage employees from sharing their login credentials with others, including individuals they may trust in their home.
- Do individuals, such as kids or significant others, have separate computer accounts on the systems? These systems are at an increased risk of exposure to malware.
- If you allow printing from home, provide protocols for protecting and disposing of printed material.
- Ensure employees have mandatory hard-drive encryption.
- Ensure data on your employees' devices is backed up on a regular basis and centralized on the company's systems. This will mitigate risks associated with Ransomware.
- Request that laptops be stored in a secure area when not in use.

Maintain Security Awareness

AAFCPAs advises clients to customize their IT Security Awareness Program for remote users to ensure your employees are mindful of security threats and avoid common pitfalls. Employee vigilance is the most effective component in keeping your data and systems secure. Phishing simulation software does a good job at identifying those who need training, and in many cases automatically directs them to training.

Companies transitioning to more remote work, either in response to the pandemic or growing employee demand, must respond to the unique security challenges involved in managing a mobile workforce. AAFCPAs' Business & IT Consulting practice advises clients on data and systems security to mitigate the risks of serious problems like identity theft, data breaches and data loss.

Contributors

Partner, Business Process & IT Consulting

James Jumes, MBA, M.Ed.
774.512.4062 | jjumes@aafcpa.com

Manager, Business & IT Consulting

Vassilis Kontoglis
774.512.4069 | vkontoglis@aafcpa.com

Certified Ethical Hacker

Mr. Anderson, MCSE, CCNP, CISSP, CEH
774.512.4066 | manderson@aafcpa.com

Chief Information Officer

Peter Sebilian
774.512.4183 | psebilian@aafcpa.com

AAFCPAs' Business Process & IT Consulting

AAFCPAs' integrated Business Process & IT Consulting practice strengthens the links between technology, processes and finance, and drives sustainable change and valuable process improvements.

Our team includes technologists with a broad understanding of business, making us uniquely qualified to advise clients on making sound business decisions regarding business processes, IT systems performance, and internal controls.

We have a comprehensive understanding of how all the pieces of infrastructure, development, data processing, security, and regulatory compliance should best fit together. Our impact has been known to make innovation real, raise the return on investment of technology, and expand IT's impact on the performance of your business.

We apply a pragmatic, business perspective to every IT investment, and focus on making a competitive difference, increasing productivity, generating new revenue, and reducing costs.

- Cyber Security
- Technology Risk Assessments
- Business Process Improvement
- Internal Controls
- IT Systems Selection & Implementation
- System and Organization Control (SOC) Reports
- Business Continuity Plans

About AAFCPAs

AAFCPAs is the premier CPA and consulting firm based in New England and considered an attractive alternative to national CPA firms by discerning clients who appreciate exceptional value. We provide audit, tax, accounting, and advisory solutions to nonprofit organizations, commercial companies, and wealthy individuals/estates. Since 1973, our sincere approach to business and service excellence has built a thriving 240+ member firm driven by an altruistic mission to improve the economic well-being and quality of life for all our constituents. AAFCPAs donates 10% of its net profits annually to nonprofit organizations.

AAFCPAs is an independent member of PrimeGlobal, the fourth largest CPA firm association in the world with 300+ member firms in 80+ countries. This provides our clients with seamless national and global coverage, along with an advantageous pay-as-you-use model.

www.aafcpa.com

clientrelations@aafcpa.com

508.366.9100