IMAGEQUEST℠ AICPA SOC

THE TOP 12 BEST PRACTICES YOUR MSP SHOULD FOLLOW, ACCORDING TO GLOBAL EXPERTS

Does your organization rely on an IT vendor, including an IT Managed Services Provider?

If so, the U.S. government wants you to take a new look at your chosen company, especially if they provide mission-critical services. If your Managed Services Provider (MSP) has the keys to your kingdom, be aware: MSPs are now a top target for cybersecurity attacks.

Last year, MSPs were put on notice when attackers breached a Kaseya MSP platform, leading to malware in their software updates for hundreds of Kaseya customers. This "supply chain" attack was the worst-case scenario for all MSPs. In May, several global Cybersecurity Agencies, including our U.S. Cybersecurity and Infrastructure Security Agency (aka CISA), the FBI, and the National Security Agency (NSA), released a joint advisory regarding MSP security.

The advisory [you can access here] details what customers should consider when choosing to work with a third-party Managed Services Provider. The advisory notes that the United States, the U.K., Canada, New Zealand, and Australia have seen "an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue."

The advisory contains 12 practices your MSP should follow to ensure they provide the best cybersecurity measures for your organization.

1. PREVENT INITIAL COMPROMISE

This broad and obvious measure includes hardening VPN access, using Vulnerability Scanning, protecting internet-facing devices, defending against brute-force and credential-stuffing attacks, and halting phishing attacks.

At ImageQuest, we have reduced our attack surface while enhancing our security and detection capabilities. We implement Zero Trust measures for remote access to our systems, applying the Principle of Least Privilege (PLP) to govern access to systems and data. We require multifactor authentication when our Single-Sign-On measures don't apply, and most importantly – we have moved our critical applications to Cloud-hosted environments. Attackers must first penetrate the application provider's Cloud security if they want to go after our critical applications. We consistently review our application providers' security measures.

We deploy a series of cutting-edge or "next generation" Detection and Response tools designed to monitor and alert across our on-premises and Cloud infrastructure. We also have an in-depth vulnerability management program that includes daily scans and real-time remediation across our enterprise. Additionally, we use the world's most recognized security awareness training platform to continually measure and improve upon the efficacy of our employees' cybersecurity maturity.

2. ENABLE OR IMPROVE MONITORING AND LOGGING PROCESSES

This measure allows rapid detection of intrusions and attacks. Early detection is a key element of a properly designed cybersecurity program. Also, monitoring can detect when malware is causing unusual behavior, such as opening a port to transmit data to an address in another country, which could signal the early stages of an attack.

ImageQuest uses a top-rated Endpoint Detection and Response (EDR) platform to monitor all devices connecting to its networks. In addition, we subscribe to a Security Operations Center (SOC) service, which uses Artificial Intelligence to scan the thousands of system logs generated daily and spot anomalies. The SOC team assesses alerts for a level of risk, using a combination of machine learning and human engineering expertise.

3. ENFORCE MULTIFACTOR AUTHENTICATION (MFA)

Today, multifactor authentication is considered an essential security measure; the cyber equivalent of locking your car in the parking lot. By now, using multifactor authentication as part of your account login should be a habit. The FBI and Microsoft estimate that MFA stops ninety to ninety-five percent of attacks.

ImageQuest uses Microsoft's Azure Single-Sign-On (SSO) service to access most of our business applications. Single-Sign-On is a sophisticated tool that incorporates multifactor authentication with identity management. We utilize SSO everywhere possible, and when it is not an option, we require MFA.

4. MANAGE INTERNAL ARCHITECTURE RISKS AND SEGREGATE INTERNAL NETWORKS

Your critical systems (e.g., servers, firewalls) should not be on the same network as your users' computers. Many refer to this as network segmentation, or you may have heard it referred to as VLAN or virtual local area network. You are making it more difficult for a bad actor to move inside your network and get to your most critical systems and data.

Another way to segment your data is to move some or all to Cloud service providers' infrastructure or SaaS (Software-as-a-Service) platforms. ImageQuest has followed this path, relying on our Cloud partners to help mitigate our risk.

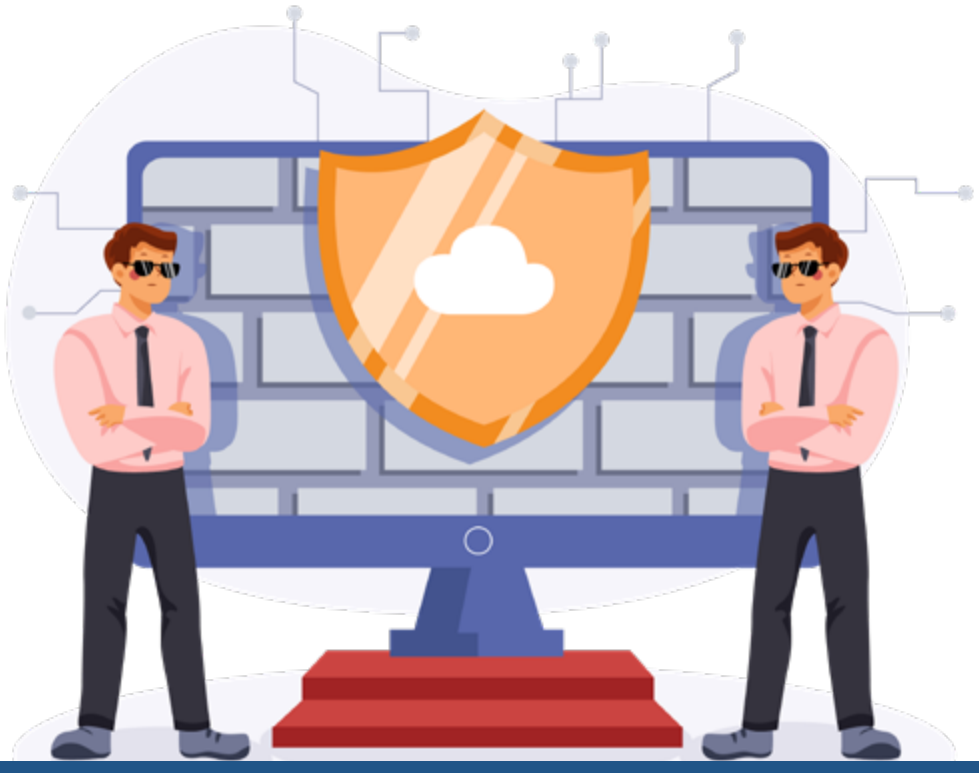
5. APPLY THE PRINCIPLE OF LEAST PRIVILEGE

Least privilege is a model that limits user access to ONLY what they need legitimate access to do their work. For example, an entry-level Help Desk technician doesn't need access to a company's backup and recovery systems. Thus, their access is restricted. Least privilege can also define and limit what service accounts (Microsoft or equivalent software) can access [A service account is a user account for the sole purpose of running background operations on a Windows server.] For example, the backup account may not need to install software to perform the backup service or routine. Therefore, you would limit the ability for this account to download or install software only.

This is a more time-consuming approach, requiring custom settings on each user and service account. However, the advantages of this approach are significant security "hardening" of your system, better stability (less chance of an unauthorized update causing a system crash), and easier application deployment with fewer access privileges.

At ImageQuest, least privilege means, for example, only our Chief Technology Officer and one other designated individual can enable or disable ImageQuest email accounts. Other managers must go through the service ticketing system to request changes to email accounts.

Least privilege also means we do not have global access to clients' systems and applications. For example, suppose we don't manage a client's payroll software, but manage the software's access to the client's firewalls and servers. In that case, our access is restricted on the payroll system, but not on the network infrastructure.



6. DEPRECATE OBSOLETE ACCOUNTS AND INFRASTRUCTURE

Disabling and removing unnecessary accounts reduces your risk by limiting your attack surface. The same holds for obsolete network equipment, servers, and computers. This is a scenario where the Cloud offers clear advantages. When your Cloud vendor manages updates, patching, and security, you don't have to spend time managing software updates and security patches. The vendor manages those updates as part of their service, and when they update the system or application, every user accessing the cloud application gets the latest version. Continued use of out-of-date legacy software and equipment leaves organizations exposed to known vulnerabilities that often cannot be fixed or patched.

Organizations should also remove accounts tied to workers no longer employed, software no longer used, and processes no longer relevant or followed.

In compliance with SOC2 standards, ImageQuest reviews our Active Directory each month to audit authorized user and system accounts, paying particular attention to accounts with elevated privileges. We refresh company laptops every three years, but moving to the Cloud has eliminated the server replacement cycle.

7. APPLY UPDATES

Your organization must establish strict policies and procedures regarding updating and patching systems and software. Procedures should include alerts reminding users to leave their devices in certain states during update windows, and there should be alerts for failed or incomplete updates. Updates should address software, operating systems, applications, and firmware. The advisory states you should prioritize updates that address exploited vulnerabilities ahead of “researcher-discovered” vulnerabilities, but you should still update for all.

ImageQuest has transitioned to daily patching schedules to match the speed with which Zero-Day attacks can move. We use applications that check for and apply relevant updates for common applications such as Chrome, Adobe, and Zoom in addition to the standard Microsoft updates. We also run daily vulnerability scans on our endpoints and infrastructure systems and regularly review those reports. Additionally, we conduct regularly scheduled Health Checks on our systems and review real-time reports from our Arctic Wolf log aggregation platform. Our Information Security Advisors assess our system reports, and provide a monthly written review just as they do for our clients.

8. BACKUP SYSTEMS AND DATA

This should actually say Backup and **test**. The gold standard is a backup file that is stored securely offline (or "air-gapped") from the rest of your systems, and you should know you can recover from it because you have tested it.

You should set up your backup system to run as frequently as necessary to allow your organization to recover rapidly when needed. Ideally, backup files should include system configurations and critical business data. You should store backup data in a readily accessible location separate from your system, such as the Cloud. The best practice is to always have three copies of your data: one in production, one in a local, rapidly accessible backup, and one stored securely offsite, separated (air-gapped) from your production systems.

When ImageQuest moved to a Cloud environment, we transferred the backup workload to our Cloud application providers. We no longer store any business or client data onsite. We are implementing a new application that can automate client configurations to reduce recovery time. As more of our clients follow us into the Cloud, fewer will need backup services for an onsite server. Their Cloud-based application providers will back up their data as part of their service.

9. DEVELOP AND EXERCISE INCIDENT RESPONSE AND RECOVERY PLANS

Every organization should know how their team will or should respond in case of a fire, flood, or cyber-attack. Your business should have an Incident Response Plan and a Disaster Recovery plan, and both should be tested in simulations and updated periodically. Contacts, systems and processes, and communications methods change. Auditors and regulators recommend you use a third-party expert to run test simulations to ensure the best results in a real-world scenario. We recommend housing digital copies in at least two different platforms along with at least one hard copy that won't be unavailable should you have no access to your digital assets.

ImageQuest's Information Security Advisors regularly conduct in-house simulations to test our Disaster Recovery and Incident Response plans.

10. UNDERSTAND AND PROACTIVELY MANAGE SUPPLY-CHAIN RISK

In cybersecurity, this refers to attacks on vendors who serve many customers, or organizations providing a critical market need. In this type of attack, the bad actors use the vendor's legitimate software update process to push their malware to client systems. The best practice for managing this risk is to thoroughly vet your vendors' security through a robust Vendor Management program.

At ImageQuest, our Information Security Advisory team manages our Vendor Management program and regularly reviews our vendors' security postures. Our team also evaluates potential new vendors to ensure we are comfortable with their cybersecurity practices before we sign an agreement and use their services.

11. PROMOTE TRANSPARENCY

In any business relationship, you should be clear about the value you receive for your investment. With an MSP relationship, transparency should include response time, uptime, and those responsible for taking specific actions if there is an incident - security or otherwise. The MSP's Managed Services and Service Level Agreements should contain these elements.

Our clients sign Managed Services and Service Level Agreements with us. We communicate with clients as changes dictate, including global threats, newly identified vulnerabilities, or new and better systems and tools.

12. MANAGE ACCOUNT AUTHENTICATION AND AUTHORIZATION

This is a special call-out to ensure you monitor login activity to your network and critical systems. Cybersecurity experts say unexplained failed logins after a password change can be the first clue that an intrusion has occurred.

This step is also a reminder not to give global access to anyone, including your MSP, unless they need that access to perform their duties. You/the MSP should restrict access based on the Principle of Least Privilege (PLP), limiting users' access rights to only what is required to perform their designated tasks.

You, the customer, should regularly audit an MSP's access to ensure it is limited to what is needed to manage your systems and account effectively.

13. WHAT THE ADVISORY LEFT OUT!

In our opinion, organizations in regulated industries – or serving regulated clients – should look for MSPs that meet the rigorous measures of a SOC2 Type II attestation. SOC, which stands for System and Organizational Controls, is a framework developed by the American Institute of Certified Public Accountants (AICPA) to provide a regular, independent attestation of the controls a company has implemented to mitigate information-related risk.

In our annual SOC 2 audit, ImageQuest describes the policies, procedures, and systems we have in place to protect information across the Trust Services Criteria categories. Our independent auditor evaluates the evidence we supply for the controls in each category. When completed, we receive our official SOC 2 report that we can share with our customers to assure them that we will handle their data securely.

Lastly, we believe adequate cyber insurance coverage is a must for MSPs. Cyber liability insurance is a risk management investment that informs and protects your MSP against devastating losses. Be sure to request a copy of their cyber insurance declarations and review them as part of your due diligence process.

TERMS

1. ***Managed Services Provider (MSP)*** – Small- and medium-sized businesses, non-profits, and government agencies typically hire an MSP to proactively manage and monitor the health and performance of the computer network and infrastructure. Entities hiring MSPs may have in-house IT staff but need additional help with projects, upgrades, or industry-related regulatory compliance issues. Other organizations turn this work over entirely to an outside company, which provides everything from computers and other equipment to cybersecurity protections and help desk support. The outsourced work is governed by a Service Level Agreement between the MSP and the Client. Many MSPs can provide IT support and security measures, but most currently do not offer regulatory IT compliance services as ImageQuest does.

2. ***The U.S. Cybersecurity and Infrastructure Security Agency (CISA)*** – The U.S. Cybersecurity and Infrastructure Security Agency, often called CISA, "leads the national effort to understand, manage, and reduce risk to the digital and physical infrastructure Americans rely on," according to CISA.gov. CISA has two key roles. One is responsibility for federal government cybersecurity, including any federal organization on the Web using a ".gov" web address. CISA also directs the response to significant cyber incidents and works to share "timely and actionable information" to federal, state, and private sector organizations.

   CISA's second role is to coordinate the defense of critical infrastructure – think power plants, water treatment, flood control, and other facilities – and ensure hackers cannot alter their operations.

   The Agency's overarching mission is to bring together public and private sectors, plus industry, academic and international experts in cybersecurity to build collective expertise on how to defend U.S. infrastructure and organizations against cyber and physical attacks.

3. ***Cloud*** – Cloud computing generally refers to remote servers at data centers worldwide. These remote servers typically host applications and related data (customer records, related files, etc.) instead of customers storing it locally on their servers. Cloud computing is popular because it gives users access to the same, latest version of software, provides resources based on need (versus being limited to what's been purchased), provides redundancy in case of disaster, and provides strong security beyond what an individual customer may be able to accomplish. The need to refresh and secure on-premise equipment is significantly reduced.

TERMS CONT.

4. ***Supply-chain attack*** – A supply-chain attack in IT is where a network system within a vertical market is compromised by attackers, often through software updates. The network may be owned by a vendor supplying advertising and marketing, accounting services, payroll, data storage – anything a company hires another entity to provide. Once the outside entity is infected by malware, attackers can send the malware to the vendor's customers. Recent supply-chain attacks include a file transfer program used by Kroger and a software company supplying IT system updates to MSPs (the latter did not affect ImageQuest.) The shutdown of Colonial Pipeline, leading to a gasoline shortage, was a different kind of supply-chain attack.

5. ***VPN*** – You may be familiar with Virtual Private Network, especially with many security software programs offering VPNs. VPNs have been around since the late 1990s when businesses supplied them to remote workers needing secure access to the company network. During the pandemic, companies discovered the limits of this 26-year-old technology, as many more people working from home than anticipated used it all at once, stalling productivity. Also, some VPNs weren't updated and were breached as a result. Companies, including ImageQuest, are moving to new remote access software.

6. ***EDR*** – Endpoint Detection and Response security software continually monitors a network "endpoint" - a laptop, cell phone, security camera, or other Internet-connected device – to detect intrusions and unusual behavior indicative of a breach. This software will alert a network administrator when a problem is detected and may provide the device user with directions on how to stop and repair the issue. The software requires the installation of a monitoring agent, and it may be company policy that the monitoring agent be installed on a device before it can access the company network.

7. ***Researcher-discovered*** – Not all vulnerabilities are discovered through security breaches or ransomware attacks. Some are found by researchers who make a living probing networks and systems for weaknesses. Some software companies pay bounties to people who find and report these weaknesses.

8. ***Air-gapped*** – Air-gapped refers to keeping a backup copy of your data and software configurations offline, separate from any connections to the internet. This practice prevents hackers from encrypting backup files that may be stored online or in a Cloud environment. If you update your air-gapped backup copy frequently enough, you have a chance of recovering faster from an attack that locks up everything else.

TERMS CONT.

9. ***Serverless Environment*** – While you may have grown up in an era with a server room or network closet, a serverless environment eliminates the physical servers at your company's location. This is achieved by moving to a fully Cloud environment (and redundant, robust Internet service.) For example, your bookkeeping software stores your company information, formulas, rates, pricing – and customer information – on its servers. When you log in, you are accessing your information on their servers, likely redundantly housed in multiple data centers throughout the U.S. Nothing is stored on a server in a closet at your company. This allows business continuity when your location suffers damage – storm, fire, power outage, etc.

10. ***SOC 2 Type 2*** – The American Institute of Certified Public Accountants developed this widely accepted framework that assesses an organization's cybersecurity controls. Company practices and policies are audited for suitable controls for information security, availability, processing integrity, confidentiality, and privacy. The SOC 2 report focuses on Service Organizations, such as an MSP, and Type 2 covers a year of operations versus the Type 1's assessment of a day of operations.

11. ***SOC-as-a-Service*** – A Security Operations Center (another SOC abbreviation!) typically monitors computer systems and the log files they generate. A log file notes every action taken on a system, including when you log in, open a program or visit a website. Logs also record the behind-the-scenes operations of your system.

    Since a computer network can generate thousands of logs daily, a SOC uses Artificial Intelligence and Machine Learning to decide which unusual log instance is a safe event and which is a security problem. The problem log alerts are then reviewed by security engineers to further winnow down irregularities that may be actual potential security incidents. The engineer then alerts the appropriate contact for the affected organization.

    A SOC-as-a-Service provides a subscription model that can be more cost-effective for organizations needing this intensive security monitoring.

12. ***Single Sign On*** – Single Sign On is an access system that verifies users once but provides access to multiple products. An everyday example is Google. Once you sign in with your Google credentials, you can access Gmail and other Google services, such as Drive, Maps, YouTube, and the Play store. You are logged out of all when you sign out of one service.