OHIO PLAN

Cyber Security Best Practices
2021

Table of Contents

Network Security Best practices

IT Support

It is becoming increasingly difficult for any small-to-medium sized organization – including public entities - to rely only upon internal IT support personnel to carry out the full breadth of services that may be required. Contracting with a trusted managed services provider (MSP) for specific IT administration needs (e.g., firewall and intrusion detection/prevention system management) can be an effective way to augment your organization's capabilities.

Identification of All Devices on Connections

An organization must identify and track the continuing presence of all computing devices (workstations, servers, network equipment, mobile devices) that are owned by an organization and permitted to interact within the organization's network environment.

Firewalls

Any organization with an Internet connection must have an actively managed firewall solution that segregates the organization's internal network from the rest of the Internet. One of the most important functions of a firewall solution is the ability to define and enforce which types of Internet traffic/services may enter the organization – including limitations on traffic coming from or going to specific Internet destinations (i.e., IP addresses & domains).

Anti-virus and Endpoint Detection and Response Software

A proper "multi-layered" cyber defense for any organization must include a contemporary anti-virus or more complete endpoint protection solution installed on individual workstations and other end-user devices. It must also be configured to continuously receive and deploy updates to reflect evolving exploit threats from bad actors, including for protection against ransomware attacks.

Updates and Patches

One of the easiest ways for bad actors to attack an organization's network and systems comes from IT administrators not being actively involved in the continuous updating/patching of their systems. As systems continue to remain unpatched over a period of time, additional new exploits are developed and aimed at out-of-date systems. An automated patch management solution that regularly deploys vendor software updates represents a key capability that your organization must have and maintain.

Secure Wireless Network

Wireless ("WiFi") networks can be a powerful tool within your organization's overall environment, but they must be protected from unauthorized access via "network sniffing" and other exploit attempts. For this reason, strong WPA2 level encryption must be deployed in all internal WiFi segments (including for "public/guest" segments that only permit access to the Internet).

Mobile Devices

Mobile devices (smartphones, tablets, etc.) that are properly authorized to access organizational applications and files represent some of the most powerful IT capabilities available to employees and management today. That said, organizations must take control of access through a contemporary mobile device management (MDM) solution that governs which devices/users can access an organization's network, systems, and applications. In particular, organizations must carefully consider the extent to which employee-owned devices are included as part of a bring-your-own-device (BYOD) company policy – and then rigorously enforce access restrictions permitted for these non-organization owned devices.

Disposal of Assets

Access to an organization's business-critical applications and other IT resources represents a key requirement for many employees in performing their assigned tasks. Within this context, IT administrators and business unit managers must join together in defining and enforcing role-based assignments for users accessing systems and applications. Enterprise-wide platforms such as Microsoft's Active Directory enable such capabilities, and must be managed on an ongoing basis to ensure that access rights updates for employee additions, terminations, and job changes are reflected promptly

Software Installation

Organization-owned workstations are not the province of their employees' imagination in terms of picking and choosing what software they want to install and use. IT administrators need to take control of organizational workstations (and servers) by disabling the ability for users to install their own software – which can often be riddled with cyber exploits (trojans, ransomware, etc.). Software distribution and implementation needs to be restricted to IT administrators who are charged with responsibility for maintaining organizational workstations and other IT assets.

USB Ports

USB ports on employee workstations are often the source of entry for trojans, ransomware, data-capturing agents, and other malware. They are also often the source of exit for sensitive organizational data in the hands of an ill-intentioned employee or contractor. USB ports should be disabled for all normal uses - except as absolutely necessary for critical business purposes – such as for the installation of approved software images.

Passwords

Strong password composition and change rules are a long-standing foundation of cyber security protection practices. Additionally, the use of contemporary multi-factor authentication (MFA) capabilities is recommended for access to highly sensitive data and/or IT administrator level privileges.

Back-ups

An organization's data backup regimen is critically important - not just for reliable recovery in the event of natural disaster, but also in case of malicious cyber-attacks that result in ransomware encryption or other data loss events. Ideally, an organization's backup regimen should include multi-generational retention, as well as a combination of both cloud-based and physical off-network storage elements.

Data Protection Best Practices

Information Asset Inventory

Organizations need to know where their sensitive and confidential information sources exist throughout all portions of their enterprise, both within paper and digital form. A well-maintained information asset inventory is a necessary pre-requisite to being able to define data protection requirements and implement necessary technology solutions for each information asset.

Information Classification

Information assets need to be classified – usually based upon a 2-to-4 tier set of definitions – according to the level of sensitivity or exposure risks that exist. Personally Identifiable Information (PII) and HIPAA-defined Protected Health Information (PHI) are well-known examples of highly confidential data that merit the highest tier level of protection.

Access Limits

When considering which employees require access to your organization's most sensitive/confidential information sources, it is essential to map essential job task requirements to well-defined role-based assignments to view/change data – rather than simply assign access rights to individual employees based upon subjective "trust factor" decisions. These role-based assignments need to be repeatable, regardless of the actual named individuals to whom these access rights may be given. When an employee's job role changes, or when the employee leaves the organization, defined procedures must be carried out on a timely basis to adjust or revoke the employee's role-based access rights.

Encryption

Contemporary cyber security standards – as well as many regulatory mandates – require that sensitive sources of information (such as PII, PHI, or PCI payment information) be fully encrypted while sitting in storage in any of your organization's servers or other repositories.

Financial Transactions and Banking Best Practices

Internal Control Systems

Any tasks within your organization that involve the movement of funds via any electronic means (ACH, wire) must be fully documented as a matter of meeting basic financial auditing requirements – in addition to ensuring that such tasks are carried out by your employees in a consistent manner.

Public Fund Transfers

Standard practice within financial institutions and other organizations includes having more than one pair of eyes approve electronic transactions, often when they rise above a pre-determined threshold amount (e.g., $1,000). A malicious cyber-attack method called "spear-phishing" involves the bad actors seeking out circumstances in organizations where a single individual has sole control over the disbursement of funds – and who might be susceptible to an illicit (but authoritative-looking) request to send money to an external bank account.

Multi-factor Authentication

When significant monetary assets of an organization can be transferred electronically with little effort (and proper authorization), organizations need to seriously consider adding more than just password access to the systems/applications that facilitate these types of transactions. The usual case involves multi-factor authentication (MFA), which might include – for example – a strong password along with a separate PIN number sent to the employee's smartphone upon request that must both be entered correctly before access is granted.

Email Security Best Practices

SPAM

Your employees receive all manner of email from any number of possible sources, both within your organization and outside of it. The use of an effective SPAM filter, often implemented as part of a mail service such as Microsoft 365, can identify emails that are known/suspected to represent malicious exploit attempts – and remove them from the mail server before they reach your employees' mailboxes.

Email Message Encryption

When an organizational employee sends sensitive/confidential information outside of the organization (or sometimes even within it, depending on confidentiality requirements), contemporary security practice requires that such information be sent in encrypted format so that unauthorized individuals may not view the contents – either by "snooping" traffic on the Internet, or while the email sits in a destination mail server waiting to be read by the intended recipient.

Email Usage Policy

Employees in your organization cannot be held legally accountable for violations of your email policy if the policy doesn't exist. Ensure that your employees are made aware of the key requirements in the organization's email policy as part of their initial orientation sessions.

Email Retention Policy

Depending on the nature of State or Federal regulations that might apply to your organization's activities, you may be subject to mandatory email retention requirements – and your IT department must work to meet them. Beyond that, however, the more basic requirements of available storage capacity within your organization may compel consideration of such a policy and its enforcement.

Employee and Computer Information Security Training Best Practices

Computer Usage Training

New employees entering your organization may come from many walks of life, with some savvy to the ways of technology and others not. A formal, uniform employee information security training program represents an essential element in equipping your workforce to be prepared for the risks associated with cyber-related activities. While on-boarding sessions covering information security practices are absolutely essential, it is also important (and often mandatory, in the example case of HIPAA healthcare-regulated activities) that employees receive ongoing guidance and support with updated information security modules, email bulletins, and periodic team discussions.

Email Usage Training

The content of your organization's emails collectively reflects the integrity, effectiveness, awareness, and reputation of your team to the outside world. Teaching employees how to properly use email services, especially for such tasks as transmitting sensitive information required by an external entity, represents an essential skill set within today's business environment.

Cyber-attack Training

Because fraudulent email represents such a significant and ongoing source of malicious attack attempts against your organization, it is absolutely essential that your employees be made fully aware of the risks involved. In today's environment, periodic testing of your employees via a commercial "phishing test" vendor represents a valuable resource that should be considered.

Policy Best Practices

Cyber Security Policies

Cyber security Policy topics reflect the need to address many of the issues covered in this online survey. If your organization's internal HR, compliance, and legal teams do not have the right experience to craft policies in these areas, management should consider investing in expert vendor guidance in the cyber security area to assist.

Data Privacy Policy

Apart from the above-mentioned Cyber Security Policy examples, the importance of an effective Data Privacy Policy represents a critical standalone component. This policy needs to reflect regulatory mandates imposed by Local, State, and U.S. authorities with respect to citizens' data privacy rights in the context of their interactions with your organization – as well as your organization's obligations to protect their private data from unauthorized disclosure to third parties. This policy requires legal participation in the creation, approval, and enforcement contexts

Vendor Security Policy

Interactions with third-party vendors represent a particularly impactful activity for an organization working to prevent and/or mitigate cyber security incident and data privacy exposure risks that exist within the context of such relationships. In order to minimize these risks to the greatest extent possible, your organization needs to develop and implement a vendor security management program that properly evaluates your vendors' handling of sensitive information on your behalf and ensuring that such practices meet the same levels of protection enforced within your own organization. Such a program may involve requesting the completion of vendor security questionnaires, conducting interviews with key vendor security personnel, performing site visits of vendor data centers, and ensuring that vendor agreements with your organization properly protect your financial and reputational interests via indemnification requirements in the case of a vendor causing an information security incident or data privacy breach that negatively impacts your organization and/or your citizens/clients.

Documented Plans Best Practices

Incidence Response Plan

Every organization must maintain a fully documented and effective Incident Response Plan, in order to ensure timely handling and mitigation of any information security incident or data privacy exposure that might occur in the normal course of activity. In such cases, time is always of the essence, and an up-to-date IRP must include: (a) roles to be performed by organizational team members, (b) key vendor, insurance, and regulatory contact information, and (c) active executive level participation and oversight in managing the investigation and remediation tasks that may be required.

Disaster Recovery Plan

A fully documented Disaster Recovery Plan incorporates both: (a) the stated information availability priorities of organizational business teams, and (b) documented and confirmed IT recovery procedures to meet and fulfill them in the event of an IT network/systems/applications disruption. Such priorities are properly established and agreed to as a product of periodic business impact analysis (BIA) exercises – which often include the confirmation of available funding to pay for expected levels of service availability. The IT team, in turn, is responsible for creating and periodically testing the recovery tasks that must take place to meet the BIA commitments for resumption of network/systems/applications availability.

Data Privacy Breach/Cyber Incident Contact

In addition to reaching out to Ohio Plan representatives to enlist their available resources, it is essential that your organization maintain an updated list contacts to trusted vendors and other key stakeholders who may need to be notified soon after recognition that a cyber security incident or data privacy exposure has taken place.