Enhancing Information Security in an Unsecure World

Password protection, network management, data security and social engineering evaluations are critical to protecting valuable information against theft or malicious activity.
INTRODUCTION

It is predicted that by 2021, businesses will fall victim to ransomware attacks every 11 seconds.¹ Needless to say, hacking innovation has been on the rise. Now, due to COVID-19, even more cyber attacks and phishing attempts are causing concern for businesses across the country.

As developments continue to unfold amid the Coronavirus pandemic, the Department of Justice has continued to warn businesses and consumers that fraudsters and criminals seek to exploit this crisis for profit. According to Forbes, within the first 100 days of COVID-19 there was an uptick in spam and opportunistic detections by 26.3 percent. In addition, impersonation were up 30.3 percent and malware up 35.16 percent.² The new and potent fraud attempts remind us that all businesses are vulnerable, and cyber security is a critical component to your business’s prosperity.

The importance of security policies and standards is paramount in today’s world. By establishing a set of expectations, tangible action steps and office culture, your business will immediately be more secure. Businesses that take the time to create and enforce security policies and standards experience a stronger business continuity, clear benchmarks, and practices.

Each section of this paper (except social engineering) is made up of three levels: Basic, Moderate and Advanced. Each level progressively guides how to improve security practices. All organizations should be able to handle Basic-level suggestions without assistance. While some organizations will be able to perform the Moderate-level security practices, most organizations will need outside assistance to perform the Advanced level.

THIS PAPER REVIEWS FOUR AREAS OF CONCERN:

1. Passwords
2. Network Considerations
3. Data Security
4. Social Engineering

Within the first 100 days of COVID-19 there was an uptick in spam and opportunistic detections by 26.3 percent. In addition, impersonation were up 30.3 percent and malware up 35.16 percent. (Forbes)
PASSWORD PROTECTION

Passwords protect the most sensitive of information, everything from personally identifiable information (PII) to intellectual property (IP). An organization could lose everything it owns if one employee becomes careless with the simple task of creating a strong password. The simplest way to mitigate this risk is to enforce complex password requirements.

A STRONG PASSWORD POLICY

A strong password policy requires passwords to be eight or more characters in length, include both alpha and numeric characters with at least one special character (~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/), be case-sensitive and not contain common names, dictionary words, foreign words, date of birth or any information closely associated with the user. The organization's network should protect passwords and automatically perform password administration so only users have knowledge of their own password.

The old adage of simply taking a word and replacing regular characters with special characters e.g., password to P@ssw0|2D, is no longer recommended as computers can now do those replacements on the fly. These recent advances in password hacking techniques have led many security researchers to recommend using a combination of random words with replacements, changes or additions such as Neptune@Error101BarbequeQ. These are both easier to remember and much more difficult to for a hacker to crack.

IMPLEMENTING CHANGE POLICIES

Implementing change policies, specifically a password aging policy, helps mitigate the risks that come with keeping a password for an extended period. Users should be required to change their password at least every 90 days and should not reuse that password within 365-day period. The system administrator should have the capability to expire passwords. Once expired, the system should require the user to enter a new password if the user ID is still active. In all cases, for each password change, an audit record should be created indicating the user ID, action (e.g., change password), time and workstation or terminal identification. Password strings should not be written to the audit log.

System administrators should change their password at least every 90 days and should not reuse that password within a 365-day period.

Where possible, the system should limit the number of consecutive incorrect access attempts by a user ID to no more than three and automatically deactivate the user ID after the third unsuccessful log on attempt. The system’s action to deactivate a user ID should affect only that user ID and not disable or otherwise affect the workstation or a different user who attempts to use the workstation. In recording the number of consecutive unsuccessful attempts for a specific user ID prior to reaching the lockout threshold, the system should reset the number to zero only after a successful log on.

TWO-FACTOR AUTHENTICATION

Two-Factor Authentication (2FA) is a process designed to ensure the security of sensitive information by means of requiring users to provide two forms of identification when attempting to access an account. A study by Google revealed that 2FA helped block 100 percent of automated bots, 96 percent of bulk phishing attacks, and 76 percent of targeted attacks. Each form of identification must be separate from the other; one may be something the user knows like a

76% Two-Factor Authentication helps block 76% of targeted attacks. (Google)
password, the other may be something the user has like a one-time token, or even something inseparable from the user like a fingerprint. 2FA adds to the assurance that the person accessing the account is actually the authorized individual.

Deciding when and where to implement 2FA should be based solely on organizational risk. It is important to understand which systems and applications are at the highest risk for unauthorized access attempts and know the impact of an unauthorized user gaining access to the system. Utilizing a risk-based approach will guide the cost and implementation discussion.

The reality is that remote access systems, including web-based systems, are under unprecedented attack. The attacks are getting more persistent and more complicated. 2FA, for remote system administration by IT staff or vendors, must be enforced. After that, it’s really a business decision. One that requires more than just the IT team’s input. Have the discussion with your business unit, risk management, IT and customer service teams to determine if 2FA is the right approach. And remember, there are multiple approaches to 2FA; make sure you are using the right one to get the outcomes you desire.

**NETWORK MANAGEMENT**

As organizations have shifted most of their workforce to a work from home status, network security has become a major priority. Malicious cyber actors are taking advantage of the mass move to telework and are exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools. An organization’s network – cloud-based or on premise – is the backbone for communications between sensitive internal and external equipment. Security controls within a network are some of the most important places to restrict unauthorized and malicious access.

**FIREWALL PROTECTION**

The internal network should be protected from other less trusted zones, specifically the public internet. This is generally done through a firewall that contains access control lists, which block unauthorized traffic and allow approved routes.

**It is generally recommended to deny any inbound access to devices on your internal network, especially without proper segmentation or additional security controls such as encryption and multifactor authentication.**

The internal network should leverage private IP addresses, which get translated to the external public IP prior to leaving the organization’s network. This will help to ensure private IP information and systems are not exposed. It is generally recommended to deny any inbound access to devices on your internal network, especially without proper segmentation or additional security controls such as encryption and multi-factor authentication. “ANY” rules are typically too general and should not be used. As an example, services such as Remote Desktop should not be accessible from the internet because they can pose high security risk and should be disable immediately.

**NETWORK ARCHITECTURE**

Proper network segmentation is necessary to build a layered security approach. Sensitive systems/servers or business critical devices should be restricted within their own network or zone. Access into each network or zone should be defined by a strict whitelist. The default rule should be to deny all traffic. Only explicitly configured address objects and services should be allowed. This includes enabling egress filtering to explicitly define which services and address objects can communicate egress in addition to ingress. This ensures communication is allowed only on required channels and all other attempts will be denied.

Devices or servers that must be exposed to the internet should be placed within a segmented network zone typically called a DMZ (Demilitarized Zone). This should allow for additional segmentation from the internal network. If the system becomes compromised, it should prove more difficult for an intruder to pivot to additional resources.
Enhancing **Information Security** in an Unsecure World

**DATA SECURITY**

During this period of mass remote-working, the Cybersecurity and Infrastructure Security Agency (CISA) has recently warned organizations about video conferencing and other collaboration tools that leave businesses vulnerable to cyberattacks. Cyber adversaries, from nation-state actors to insiders and criminal organizations, seek to acquire information on research and development, critical infrastructure, and personally identifiable information. An IT policy should be used to define appropriate methods for securely transferring or sharing data with authorized recipients as well as restricting against the use of unsupported services.

**UNDERSTANDING USER AGREEMENTS**

All data sharing services have user agreements outlining their terms and conditions. These terms, once accepted, many times allow the provider varying control over accessing the content of the data stored with them. Typically, this is used to improve their services offered, but in doing so could be exposing sensitive information that was not meant to be shared. Generally, some of the free services allow the company to make your information anonymous but index the content, which could introduce compliance issues as well as expose sensitive information publicly. User agreements should be reviewed by businesses that leverage third-party software for file sharing.

**ENCRYPTION**

Sensitive data at rest or in transit should always be encrypted for maximum protection. Businesses need to qualify sensitive data and ensure proper security controls are in place to safeguard its confidentiality. This is typically performed by leveraging encryption, which renders information unreadable when accessed without proper authorization. It is imperative for businesses to establish an employee process that ensures sensitive devices are encrypted, and secure file transfers and emails are being properly distributed.

**SOCIAL ENGINEERING**

The human element in information security is often overlooked by organizations. One can have the most advanced technology in the world, but untrained employees can leave an organization vulnerable to malicious attacks.

Using social engineering, cybercriminals rely on human interaction, tricking people into breaking normal security procedures. Social engineering assessments provide a practical view into the behaviors that threaten an organization and identify how well employees are trained to follow security programs.

In an external social engineering assessment, security consultants perform exploratory research by doing what the intruder might do — utilize the internet to gather a sufficient amount of business and employee information, starting with public information that can be found on websites, social media platforms and DNS records. Employee names, job titles, phone numbers, email addresses and recent company news are gathered to conduct nefarious activities based on social engineering.

**Information cybercriminals gather to conduct nefarious activities based on social engineering:**

- Employee names
- Job titles
- Phone numbers
- Email addresses
- Recent company news
PRETEXTING PHONE CALLS

The information gathered in the exploratory phase provides a foundation for conducting introductory phone conversations. These pretexting calls gather sensitive information from seemingly helpful employees. The consultant impersonates a trusted source and makes the employee feel as if he/she is responsible for assisting them. Without proper training, the employee often divulges sensitive information used in the next phases of an attack utilizing social engineering.

DUMPSTER DIVING

For example, dumpster diving isn’t a glamorous part of the job, but it is a very realistic element of an attack. Consultants rummage through unlocked trash and recycling bins to discover valuable information that could be used in a malicious attack. Sometimes the simplest oversights, like forgetting to shred a sensitive document, can leave an organization vulnerable to attacks.

PHYSICAL ENTRY, ONSITE SECURITY AND SOCIAL ENGINEERING ASSESSMENTS

These assessments look at onsite opportunities to gather sensitive information about the company. This is where there is testing of building access controls, IT asset controls and employee behavior, and may include testing of physical security systems like locks and card-key access, reactions to unescorted visitors and unattended computer workstations.

Security consultants perform physical security assessments by attempting to enter premise through piggybacking (walking through a slowly closing door), simply asking an employee to hold the door open, or posing as a vendor or repair technician. Once in the building, our consultants attempt to access data centers, executive suites, file rooms or other restricted access areas. Our goal is to gather employee logins (many people use Post-It notes to remind themselves of their own login credentials), take photos of conference room schedules or conference call access codes, or plant technology devices, which can be used to remotely hack your company from the inside.

CONCLUSION

The best tools for organizations to be protected is to be purposeful and vigilant. By assessing vulnerabilities, implementing processes and procedures to address them and monitoring ongoing compliance, organizations can mitigate exposure to COVID-related cyberattacks during these unprecedented times.

---


At Aureon, we offer reliable business solutions so our Clients can focus on their day-to-day operations. For more than 30 years, connectivity has driven our business and has been woven into the network of solutions we offer customers. From technology to consulting to contact center operations, we develop creative and customized solutions based on our knowledge and understanding of our Clients. When you connect with Aureon, you connect with solutions.