NAED
NATIONAL ASSOCIATION OF
ELECTRICAL DISTRIBUTORS

Executive Guide #15

Ten Things Distributors Can Do to Enhance Password Management and Increase Security

Developed by the NAED Strategic Technology Committee
Published January 2016

Information security is about people, mindsets, and behaviors.

Passwords protect against unauthorized account and equipment access in order to keep information private and financial accounts secure. Shared, weak, and easily guessed passwords can lead to data and system compromises, allowing cyber criminals to steal identities and wreak havoc—*if not at your company, than perhaps by using your company to access the systems of your major suppliers or customers.* **Have you ever stopped and thought about all the sensitive and highly confidential information passwords protect in your company?**

NAED's Strategic Technology Committee created this white paper to assist distributor executives in understanding password security issues and to stimulate conversations with Information Technology (IT) personnel. While not an all-inclusive listing, it focuses on the proactive steps distributor executives can take to foster better password management and use at their individual companies. Suggestions are also offered on how distributor executives can balance usability with security when determining password length and complexity. Examples will be provided from the infamous 2013 Target data breach to illustrate how easily systems can be compromised if the entire organization is not focused on information security.

10 THINGS DISTRIBUTORS CAN DO TO ENHANCE PASSWORD MANAGEMENT AND INCREASE SECURITY

1. Keep information security top-of-mind with all company associates
2. Change default administrator passwords
3. Use unique passwords for critical applications
4. Emphasize passwords are not to be shared
5. Provide company approved technical solutions for secure password management
6. Require strong passwords
7. Require passwords be changed regularly
8. Use real-time protective monitoring
9. Conduct regular searches for password information stored in plain text
10. Routinely cancel passwords when employees leave your employment

1 Keep information security top-of-mind with all company associates through straight-forward information security policies reinforced with ongoing communications and information security awareness training.[1]

More than 80% of data breaches are directly linked to people.[2] Knowledgeable associates are electrical distributors' first and best line of defense against data breaches.

Cyber criminals look for easy targets. Some try lists of easily guessed passwords. Others try to trick users into revealing passwords over the phone or with a genuine-looking email. Emails masquerading as coming from legitimate companies are often used to trick users into resetting passwords at counterfeit websites, click on a link in order to install malware, or unwittingly exploit security gaps in out-of-date software. Company associates aware of cyber criminals' latest techniques and trained in what to do if they spot suspicious activities are less likely to succumb to these tricks.

Knowledgeable associates are the best defense against data breaches.

EXAMPLES OF COMMON, EASILY GUESSABLE PASSWORDS IN USE[3]

111111
121212
123123
1234
12345
123456
12345678
1234567
123456789
1234567890
696969
abc123
access
baseball
basketball
batman
changeme
dragon
football
flower
hottie
letmein
login
loveme
master
michael
monkey
mustang
NASCAR
password
princess
qwerty
rugby
shadow
soccer
solo
superman
trustno1
welcome

WAYS CYBER CRIMINALS CAN OBTAIN PASSWORDS

→ **Phishing** *(also known as social engineering): Tricking users into---*

- *Revealing log-in information over the phone or in an email;*
- *Resetting passwords through links to counterfeit website pages;*
- *Providing sensitive information in response to fake emails;*
- *Clicking on links to install malware; and/or*
- *Downloading fake attachments.*

→ **Shoulder Surfing:** *Watching users enter their password or using a cellphone (or even a hidden camera) to record password entry.*

→ **Guessing:**

- *Trying commonly used passwords; or*
- *Using publicly available personal information to guess passwords.*

→ **Intercepting passwords over unsecure Wi-Fi at airports, coffee shops, hotels, restaurants, etc.**

→ **Installing physical key loggers or key logging software on devices**

→ **Searching devices and networks for unencrypted passwords**

→ **Brute force attacks:** *Computerized decryption trying every possible combination of numbers, letters, and special characters until a password is discovered.*

> ***REMEMBER THE MOVIE, "THE IMITATION GAME," DOCUMENTING ALAN TURING BREAKING THE GERMAN ENIGMA CODE?*** *THAT'S THE SAME TECHNIQUES CYBER CRIMINALS USE TO OBTAIN PASSWORDS."*

[1] Security awareness training is available in NAED's VIP Access Core Library as well as from companies such as Wombat Security Technologies, FireEye, and the SANS Institute.
[2] 2015 Data Breach Investigations Report http://www.verizonenterprise.com/DBIR/2015/
[3] Based on Splash Data's Annual "Worst Passwords" List and Sky High Network's Cloud Services Password Study

More advanced adversaries may use technical methods to obtain passwords. Examples include intercepting passwords sent over unsecured Wi-Fi; using hardware or software to monitor keystrokes on devices, i.e., key logging; searching devices and networks for listings of unencrypted passwords; and *"cracking"* weak passwords—*trying every possible combination of numbers, letters, and special characters until a password is discovered, i.e., brute force attacks.* Again, electrical distributors' best defense is trained company associates fortified with real-time monitoring, regular vulnerability assessments, and executives with a game plan on how to handle an information security breach—*known as a Computer Security Incident Response Plan (CSIRP).*

PCI Compliance does not automatically mean information is secure.

Payment Card Industry Compliance (PCI Compliance)

Adherence to a set of specific information security standards—Payment Card Industry Data Security Standards (PCI-DSS)—developed to protect credit card information during and after a financial transaction. The goal of PCI Compliance is to ensure merchants provide the maximum security when processing customer payments or handling customer data. PCI Compliance applies to all organizations or merchants, regardless of size or number of transactions, that accept, transmit, or store any cardholder data.[4]

NOTE: Unfortunately, PCI compliance does not automatically mean digital assets are secure. Target claimed to be fully compliant with Payment Card Industry Data Security Standards (PCI-DSS) but information for 110 million customers was still lost to cyber criminals.

Computer Security Incident Response Plan (CSIRP)

An overall plan to detect and respond to information security incidents by characterizing incidents ("what" is happening), defining the roles and responsibilities of participants ("who" does "what" "when" if "this" happens), and outlining reporting requirements.

Credentials from an HVAC contractor with access to Target's electronic billing, contract submission, and project management systems were used to gain access to Target's network. The anti-malware software used by the HVAC contractor did not provide real-time protection and is only intended for use by individual consumers, not businesses.

DO YOU KNOW?

- *How your company keeps information security top-of-mind with all company associates?*
- *What information security awareness training all company associates receive regularly?*

[4] Definition from Electrical Industry Dictionary https://www.naed.org/NAED/naed/Resources/Business_Tools/Electrical_Industry_Dictionary.aspx

2 Change default administrator passwords during initial installation of all hardware and software.

Desktops, laptops, tablets, smartphones, software, routers, switches, Point-of-Sales (POS) terminals, specialized hardware, etc. are shipped from the factory with default administrator passwords installed in order to provide technical support remotely. Sometimes in the rush to use new hardware and software, users overlook default administrator passwords and neglect to change them.[5] In other cases, default user-ids and passwords may be knowingly left in place to allow authorized third parties—*consultants, contractors, Managed Service Providers, VARs*—to provide technical support remotely.

Managed Service Providers (MSP)

Assume day-to-day management and operational responsibility for performing specified functions.

Value-Added Resellers (VAR)

Resell software, hardware and/or networking products and provide value beyond order fulfillment.

Default passwords allow individuals with malicious intent to potentially gain access to your networks too. Once inside, threat actors can assume the role of system administrator, enabling them to change default passwords in order to hold company information for ransom, steal company information, wreak internal havoc, and/or use your company to gain access another company's networks *(potentially a larger target)*.

Default passwords can allow cyber criminals to gain access to your networks.

If your company accepts payment cards, your payment processor will require compliance to PCI-DSS, which specifies *"Do not use vendor-supplied defaults for system passwords and other security parameters."* In addition, distributor executives should also require separate passwords be created for each 3rd party accessing company systems and contractually require 3rd party service providers be PCI Compliant.

The severity of the Target breach was exacerbated by the use of default passwords for key internal systems and servers allowing the threat actors to assume the role of system administrator with complete freedom to move about Target's network for months before discovery.

DO YOU KNOW?

- *Your company's process for resetting default passwords?*
- *How your company's default password process is monitored? Enforced?*
- *If your 3rd party technical support providers are PCI Compliant?*

[5] Routers, switches, and point-of-sales terminals are particularly vulnerable to those with malicious intent.

3 Use unique passwords for critical applications.

Passwords keep information private and financial accounts secure by preventing unauthorized access. Using the same password for business and personal accounts is similar to using the same key for one's car, house, and office. Yet a study by Telesign, a mobile identity solutions company, reported 73% of online accounts use duplicate passwords.[6]

Encourage the use of separate passwords for business and personal accounts.

Using the same password for multiple accounts makes it easy for cyber criminals to compromise one password to gain access to all of the users' accounts using the same password. Although it is difficult to monitor and enforce, make sure your company's Information Security Policy strongly encourages the use of separate passwords for business and personal use.[7] Electrical distributors should also contractually require authorized third parties—*consultants, contractors, Managed Service Providers, VARs, etc.*—with access to your company's systems and information, not to repeat the same password for other customers.

Access to Target's networks was gained through a small HVAC contractor with access to its electronic billing, contract submission, and project management systems. The HVAC contractor was breached through malware delivered in an email at least 2 months before Target was attacked.

DO YOU KNOW?

- *How duplicate passwords are address by your company's Information Security Policy?*
- *If your 3rd party technical support providers use unique User ID and passwords to access your networks and systems?*
- *How the systems accessed by 3rd parties are separated from the rest of your company's networks?*

4 Treat passwords as personal, confidential information, not to be shared with ANYONE.

Business passwords must be treated as private, confidential information not to be shared with coworkers. This ensures company information is only viewed by those with authorized access and protects the password *"owner"* from bearing responsibility for the mistakes of others. It also provides the physical audit trail required for PCI Compliance.

Similar to other confidential company information—*payroll, personal health information (PHI), etc.*—written passwords should not be stored near computers or in unlocked areas accessible to anyone other than the authorized user. Ideally, passwords should only be stored in an abbreviated form only the user will understand in a fireproof safe.

[6] https://www.telesign.com/site/wp-content/uploads/2015/06/TeleSign-Consumer-Account-Security-Report-2015-FINAL.pdf

[7] Some security-minded distributors monitor and enforce the use of separate passwords for associate access to ERP system information and external vendor sites.

However, co-workers sometimes feel pressure to share their passwords in order to quickly respond to customer requests. Examples of this practice include one warehouse worker seemingly entering all the receipts and/or shipments; onsite ERP log-ins from the office by associates not in the office on a certain day, etc.

Eliminate the need for password sharing by developing company-approved processes.

Distributor executives can eliminate the necessity for password sharing by providing company-approved processes. For example, the company email system may allow emails to be automatically forwarded to a designated person, a group email could be created, or shared email files enabled. Work-related files can also be stored on a shared drive available to authorized associates.

In certain predetermined cases—*such as when associates are on vacation or on medical leave*—short-term, temporary access to certain information can also be granted to designated associates. The point is to quickly respond to customer requests ***while*** maintaining authorized access to information.

SOFTWARE LICENSES

Software programs are protected by U.S. copyright law and are typically licensed for use rather than sold. The license terms are specified in the End User License Agreement (EULA) which usually appear as the terms and conditions one must accept before being allowed to use the software the first time.

A software license is usually for a given number of computers or people, whichever is smaller. For example, a distributor with 3 people using 11 devices needs 3 licenses, even if only 1 person uses the software at a time. Doing otherwise could violate the terms of your software license and subject your company to possible legal action for violating U.S. copyright law.

Security consultants brought in after the Target breach found an unencrypted file containing valid network credentials stored on several servers. This provided direct and complete access to everything on Target's network, including every cash register in every Target store.

DO YOU KNOW?

- *How authorized coworker access to information required to respond to customer requests is enabled?*
- *Your company's process for granting temporary access to an associate's email accounts and electronic files?*

5 Provide *company approved* technical solutions for secure password management.

As electrical distributors rely more and more on technology, company associates must remember, store, and otherwise keep track of dozens of passwords.[8] Distributor executives can reduce associates' password overload and reduce risky behaviors by offering company approved technical solutions for securely remembering and storing passwords. Examples of these technical solutions include single sign-on, password managers, access cards, and biometrics.

Offer company-approved technical solutions for securely storing passwords.

RISKY WAYS USERS "REMEMBER" PASSWORDS

- *Writing passwords down on "sticky notes," etc.*
- *Storing passwords on hard drives in unencrypted files*
- *Creating predictable password strategies*
- *Employing the same passwords for multiple sites*
- *Logging-in to accounts through major companies (Google, Facebook, Twitter, etc.)*
- *Not logging out at the end of each session*
- *Resetting passwords at each log-in*
- *Using easy-to-guess passwords*
- *Logging in automatically, i.e., using "Remember My Password"*

Single sign-on is an authentication process allowing a user to access multiple authorized applications with only one user name and password.

Password Managers—*also referred to as password vaults*—act as a virtual safe by securely storing and organizing users' passwords for different accounts. The user accesses the password manager with a single, "*master*" password. Some password managers can also help prevent phishing, since many only provide information based on the website's URL. And make sure your ***company-approved*** password manager includes strong encryption and authentication capabilities. Examples of password managers to consider include LastPass, KeePass, Dashlane, 1Password, and Password Box.

Digital Access Cards offer secure solutions for computers shared by several users as well as for computers in public areas, such as an electrical distributor's counter area. The digital access card allows the card "*owner*" to access authorized applications without manually entering a user name and password. Typically, as long as the user's card is inserted in the card reader, information can be retrieved and viewed. However, the user is automatically logged out when the card is removed. In other cases, the access card is "swiped" by a card reader and the user is logged out after a predetermined amount of inactivity.

Biometrics—*fingerprints, iris scans, voice recognition, etc.*—are beginning to emerge for mainstream user identification. However, expense and privacy concerns may hinder widespread implementation.

DO YOU KNOW?

- *What technical solutions your company offers for managing passwords?*
- *How security is addressed for shared computers and computers in public areas?*

[8] According to the ID Federation, there can be, on average, 40 – 50 different passwords per user for business and personal accounts.

6 Require strong passwords.

Password complexity correlates directly with password security. There is a wide variety of opinions over what constitutes a strong password. PCI Compliance requires a minimum of 7 numeric and alphabetic characters.[9] Apple IDs must have a minimum of 8 characters, include a number, an uppercase letter, and a lowercase letter, and not contain more than 3 identical characters. Apple also suggests, but does not require, adding special characters and punctuation marks to make Apple IDs even stronger.[10] The SANS Institute[11] recommends using passwords with at least 12 alphanumeric characters, with both upper and lowercase letters, at least one number (0-9), and at least one special character (!$%^&*()_+|~-=\`{}[]:";'<>?,/) for maximum protection from computerized decryption attempts.

OPINIONS ON THE COMPOSITION OF A "STRONG" PASSWORD VARY

PCi

Minimum 7 numeric and alphabetic characters.

Minimum 8 characters: a number, an uppercase letter, a lowercase letter, and not more than 3 identical characters.

SANS INSTITUTE

At least 12 alphanumeric characters: both upper and lowercase letters, at least 1 number, and at least 1 specialized character.

[9] PCI DSS Version 2.0 8.5.10 and 8.5.11.
[10] Security and your Apple ID https://support.apple.com/en-us/HT201303
[11] A cooperative research and education organization providing cyber training and certification to professionals at government and commercial institutions worldwide. www.sans.org

Password complexity correlates directly with password security.

Electrical distributors must balance usability with security when determining password length and complexity. Requiring too many characters and combinations can lead to less than secure behaviors—*easy-to-guess passwords, predictable password creation strategies, the duplicate use of passwords on multiple sites, etc.* On the other hand, requiring too few characters makes password decryption quicker and easier for cyber criminals.

Some electrical distributors solve this dilemma by requiring word sequences to log-in to company accounts, i.e., a passphrase, with numbers and special characters inserted throughout in place of letters. Others create *"blacklists"* of banned password choices.

SUGGESTED PASSWORDS TO BAN, OR *"BLACKLIST"*

Electrical distributors can enhance password security without negatively impacting usability by banning passwords containing:

- *Common words found in a dictionary, slang, dialect, or jargon*
- *Common words spelled backwards, or preceded or followed by a number---terces, secret1 or 1secret*
- *Letter or number patterns---aaabbb, qwerty, zyxwvuts, 123321, etc.*
- *Obvious information---account names, company name, computer name, user names, your name or nickname, etc.*
- *Work-related information---building names, system commands, sites, companies, hardware, software, etc.*
- *Personal information that can be gleaned online---addresses, athletes, birthdates, brand of cars, celebrities, friends, fantasy characters, family member names, favorite films, hobbies, pets, phone numbers, Social Security numbers, song lyrics, sports teams, quotes, video game titles, wedding anniversaries, zip codes, etc.*

Although Target has a password policy, it was not being followed. A report analyzing the 2013 Target breach[12] reported security consultants were able to crack 86% of Target's 547,470 passwords within 1 week---allowing access to various internal networks. In addition, 34% of Target's admin domain passwords were cracked within a week.

DO YOU KNOW?

What your company does to ensure all passwords are strong?

[12] Krebs on Security September 21, 2015

7 Require passwords be changed regularly.

The longer a password is used, the higher the chance it will be stolen or guessed. The Telesign study found 21% of U.S. respondents were using passwords over 10 years old, 46% were using passwords over 5 years old, and 30% were using passwords 1-4 years old!

Some argue frequent password expiration leads to passwords that are only minor variation of the previous version, the use of duplicate passwords across various systems, and/or use predictable password creation strategies. However, regularly changing passwords lessens electrical distributors' risk in the event of a compromise. As computing technology improves, decryption efforts *(also known as brute force attacks)* occur quicker, and rather than using stolen passwords immediately, many cyber criminals leave them unused for some time before selling them.

Regularly changing passwords lessens risk

A STUDY BY TELESIGN FOUND:

30% *use passwords over 1-4 years old*

46% *use passwords over 5 years old*

21% *use passwords over 10 years old*

Finding just the right time interval for password change requires electrical distributors balance usability with security considerations. While PCI Compliance requires users change passwords at least every 90 days, some payment card processors have even more stringent password change requirements. Some 3rd party service providers—*HR services, payroll, banks, sales tax software providers, etc.*—have stringent password change requirements too.

WHEN TO CHANGE PASSWORDS

Regularly—*Every 90 to 180 days depending on your company's needs*
Immediately upon suspicion or detection of a breach

Recommendations from the SANS Institute are a bit more lenient---change system level passwords at least quarterly and user level passwords at least every 6 months. There is universal agreement, however, on changing passwords immediately on indication or even suspicion of compromise—*if you felt like someone was watching you type it, you notice signs of strange activity, etc.*

DO YOU KNOW?

- *The steps your company takes to ensure passwords are changed regularly?*
- *Your company's process for escalating password change requests to prevent automatic system "lock-outs?"*

8 Use real-time protective monitoring to detect suspicious activity and take appropriate action in response to system alerts.

Monitoring and tracking all access to network resources and cardholder data is required for PCI Compliance. Electrical distributors can detect suspicious activity in real time by monitoring logins and usage patterns by system—*Windows, portal, ERP, etc.*—and setting limits for data transfers.

Taking the appropriate action when urgent system alerts are triggered is crucial to limiting the extent of a breach. In the aftermath of the attempted intrusion, review and evaluate the effectiveness of the preplanned actions in the company Computer Security Incident Response Plan (CSIRP)—*what worked, what didn't, what was learned, etc.*—and amend the document as necessary.

Many signals of an incursion were ignored throughout the Target organization. Although Target's FireEye malware intrusion detector system triggered urgent alerts, Target's security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware. Symantec antivirus software also detected malicious behavior on the same server as the FireEye software.[13]

DO YOU KNOW?

- *How your company monitors for suspicious activity?*
- *Your role in the company's Cyber Security Incident Response Plan (CSIRP)?*

[13] Report to the U.S. Senate's COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, A "Kill Chain" Analysis of the 2013 Target Data Breach

9 Conduct regular searches for password information stored on company equipment and systems.

Unencrypted passwords should never be sent in emails or stored in electronic files on a computer, on company servers, in the cloud, or on mobile devices since spyware programs and viruses can easily retrieve stored passwords. Even distributors using anti-virus and spyware protection software may still be vulnerable if unencrypted passwords are stored.

Instead, any stored passwords should be encrypted—*using techniques such as salting and hashing*—as required for PCI-DSS Compliance.

ONLY STORE ENCRYPTED PASSWORDS

A regular audit should be conducted to search for unencrypted passwords in electronic files, on company servers, and in the cloud. And while it may not be practical to search personal devices—*phones, tablets, etc.*—for password information, it does make sense to include a requirement about unencrypted passwords not be stored in your company Information Security Policy.

In addition, encrypted electronic and paper copies of administrator passwords and company password listings should be stored in fireproof safes both on- and off-site and set up so the information can only be retrieved by pre-designated, authorized parties in the case of a disaster.

Security consultants brought in after the Target breach found an un-encrypted file containing valid network credentials stored on several servers. This provided direct and complete access to everything on Target's network, including every cash register in every Target store.

DO YOU KNOW?

- *How often your company conducts audits for unencrypted passwords?*

10 Routinely cancel passwords and electronic access when employees leave your employment.

Whether associates leave voluntarily or are terminated, information security considerations must be a key part of every electrical distributor's off-boarding process. It is also required for PCI Compliance. Access to company systems must be immediately revoked, all passwords—*including reset capability*—immediately deactivated, and mobile devices immediately "wiped" clean of company information.

Information security is a key part of the off-boarding process.

As mentioned previously, group email accounts, shared email files, and the storage of work-related files on a shared drive enables authorized company associates to continue to respond to customer requests. Company-approved password managers facilitate cancelling passwords for internal systems as well as for external sites. Mobile Device Management software enables remote removal of data from mobile devices even if an off-boarded employee changes their password.

Mobile Device Management, or MDM

A software tool used by network administrators to remotely activate or deactivate a mobile device, authorize, authenticate, apply appropriate security, configure settings, update mobile device operating systems and software, track usage, enforce company policy and otherwise manage mobile devices, up to and including removing data from the device remotely.

DO YOU KNOW?

- *How your company's off-boarding process addresses information security concerns?*

Recommended Resources

SANS Institute https://www.sans.org/

The SANS Institute was established in 1989 as a cooperative research and education organization. It develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - *the Internet Storm Center*.

Password Construction Guidelines
https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

Password Protection Policy
https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

Carnegie Mellon University

CyLab Usable Privacy and Security Laboratory *(CUPS)*A listing of Passwords and Authentication Research
https://cups.cs.cmu.edu/passwords.html

Guidelines for Password Management
https://www.cme.edu/iso/governance/guidelines/password-management.html

Massachusetts Institute of Technology (MIT)

Strong Passwords
http://kb.mit.edu/confluence/display/istcontrib/Strong+Passwords

University of Chicago

Good Password Practices
https://itservices.uchicago.edu/page/good-password-practices

What You Can Do

While data breaches are the new normal for companies of all sizes and in all industries, a few things can make a big difference in the security of your company's information. Here are our top four suggested actions electrical distributor executives can take to decrease your company's risk of a data breach:

1. ***Prioritize information security by developing an up-to-date company information security policy.***
2. ***Embed safe computing behaviors into company culture by ensuring company associates receive ongoing information security awareness training.***
3. ***Monitor, recognize and reward company associates for integrating security awareness into the normal course of their day-to-day job functions.***
4. ***Conduct ongoing, regular 3rd party security audits to identify your information security vulnerabilities and take appropriate action in response to your findings.***

Share your insight and input with NAED's Strategic Technology Committee by calling NAED Member Services toll free at 1.888.791.2512 or emailing memberservices@naed.org.

Be on the lookout for additional tools from NAED's Strategic Technology Committee, available for download at www.naed.org/strategictechnology.

UPCOMING TOPIC: Electronic Access