NATIONAL ASSOCIATION OF ELECTRICAL DISTRIBUTORS

Executive Guide #16

Ten Things Distributors Can Do to Prevent Data Loss

Developed by the NAED Strategic Technology Committee
Published March 2016

Data Loss Prevention requires controlled access to information.

Almost every day, there is another headline about a major data breach at a well-known company. Decades ago it was relatively easy to control access to company information. Computers were locked away in rooms reachable only by a few IT people. Back-up disks were big, bulky, and often stored in fire-proof safes. Hard copies of confidential information were stored in locked file cabinets. And the typical cause of data loss was equipment failure or, in rare instances, a natural or manmade disaster.

Fast forward to 2016. Mobile technology, social media, and e-commerce have changed how electrical distributors communicate, interact, and conduct business. Everyone is connected to the Internet using multiple devices—*desktop computers, laptops, smartphones, tablets, etc.* Information must be available in real time and accessible from anywhere. Cyber criminals are also on the prowl, looking for easy targets.

Electrical distributors must take prudent steps to protect their information from its point of origin, through all points of transit, to its storage—*i.e., from **end-to-end**.* Any compromise of information—*whether accidental or intentional*—can disrupt operations; result in lost sales; damage company reputation and brand; and lead to significant out-of-pocket costs.

NAED's Strategic Technology Committee created this white paper, ***"Ten Things Distributors Can Do to Prevent Data Loss,"*** to assist distributor executives in understanding how to protect information from loss through theft, fraud, and misuse as well as to stimulate conversations with Information technology (IT) personnel about the various means to do so.

While not an all-inclusive listing, we highlight proactive steps distributor executives can take to foster better data loss prevention at their individual companies.

10 THINGS DISTRIBUTORS CAN DO TO PREVENT DATA LOSS

1. Understand where the information your company needs to protect resides
2. Carefully oversee system administrator privileges
3. Limit information access to "need to know"
4. Require strong, unique passwords
5. Protect devices accessing networks or storing information with automatic screen lock
6. Use passcodes to "unlock" screens and devices
7. Offer company-approved storage and disposal solutions
8. Provide secure wireless connections for remote users
9. Use at least two ways to authenticate systems administrators and remote users
10. Make sure information security basics are covered too

Data loss prevention requires limiting access to the equipment and software originating, transmitting, and storing information. Access to data center equipment must be physically restricted and electronically protected too. It is also required for PCI Compliance.[1] However, safeguarding office and mobile equipment by limiting electronic access is the focus of this white paper.

Access Control

Any means of limiting access to IT assets–both physical assets and information assets–by regulating who can reach them.

Protect information from the point of origin, through all points of transit, to storage—i.e., from end-to-end

PHYSICAL IT ASSETS	*Examples of Physical IT Assets include:* • **Data Center Equipment:** *Networking equipment, routers, servers, switches, etc.* • **Office Equipment:** *Desktops, copiers, printers, etc.* • **Mobile Equipment:** *Laptops, Smartphones, Tablets, etc.* • **Information Storage Devices:** *Back-up disks, CD's, "Cloud" Storage, USB's, etc.*	*Protect by:* **CONTROLLING ACCESS**
DIGITAL ASSETS *Information contained on, or accessible through, Physical IT Assets*	*Examples of Digital Assets include:* • **Company Information:** *Financial, pricing, products, website, etc.* • **Customer Information:** *Financial, pricing, etc.* • **Employee Information:** *Healthcare, payroll info, etc.* • **Supplier Information:** *Financial, pricing, products, website, etc.* • **Company Approved Operating Systems and Software**	

[1] PCI-DSS compliance is required of those distributors accepting credit cards. Requirement 9 covers restricting physical access to cardholder data. Additional information is available @ https://www.pcisecuritystandards.org/

1 Understand where the information your company needs to protect resides.

Protecting company data from end-to-end begins with inventorying all the devices and software used to originate, modify, transport, and store data on the company network to determine your vulnerabilities. Most IT Disaster Recovery Plans include equipment and software inventories, so you may only need to update it.

Inventory all devices and software originating, modifying, transporting, and storing data on the company network

EXAMPLES OF WHERE DATA CAN RESIDE AT A TYPICAL ELECTRICAL DISTRIBUTOR

COMMUNICATION TECHNOLOGY

- *Email*
- *Instant Messenger*
- *Telephone (Landline, VOIP, etc.)*
- *Text Messaging*
- *Voice Mail*
- *Web conferencing*

PORTABLE OFFICE TECHNOLOGY

- *Company - internal apps*
- *Contact note applications*
- *Laptops*
- *Mobile Device Management (MDM)*
- *Smartphones*
- *Tablet Computers*
- *Vendor apps*
- *Voice transcription applications*

BACK OFFICE TECHNOLOGY

- *Electronic Data Interchange (EDI)*
- *e-signature (Proof of Delivery)*
- *Truck Routing Software*
- *Bar Coding/Scanning*
- *GPS Vehicle tracking*
- *VDP Voice Direct Picking (VDP)*
- *Vendor managed Inventory (VMI)*
- *Warehouse Management Systems (WMS)*
- *Wireless Inventory Control (RFID)*

IN OFFICE TECHNOLOGY

- *Business Intelligence & analytics software (BI)*
- *Cloud-based collaboration software*
- *Cloud storage services*
- *Company website & Ecommerce capabilities*
- *Customer Relationship Management (CRM)*
- *Online training*
- *Password managers*
- *Sales force automation (SFA)*
- *Sales performance & productivity applications*
- *Social Media (for communicating inside the company)*
- *Time tracking software*

CUSTOMER FACING TECHNOLOGY

- *Apps for customers*
- *Blogs*
- *Digital signage*
- *Ecommerce Website*
- *Email marketing tools*
- *Interactive Videos*
- *Mass texting*
- *Punch-out Integration*
- *Social & keyword trackers*
- *Social Media (External to the company)*
- *Surveys*
- *Vendor managed Inventory (VMI) for customers*

If your company doesn't have an IT Disaster Recovery Plan, begin with a listing of the IT assets the accounting department is depreciating, then survey company personnel, before expanding the listing to include personal and portable devices. Or you can compile a listing manually by "sweeping" your networks periodically and comparing changes.

Commercially available tools to automate device and software discovery and automatically keep the device inventory updated include Nagios, PRTG Network Monitor, Spiceworks, Wireshark, etc.

FOR MORE INFORMATION:

- *Executive Guide #8: IT Disaster Recovery Planning — http://www.naed.org/NAEDDocs/Research/Benchmarking/IT_Disaster_Recovery.pdf*
- *Sample computer equipment and software inventory forms — http://disastersafety.org/wp-content/uploads/6-Know-Your-Information-Technology.pdf*

2 Carefully oversee System Administrator privileges.

System administrators are entrusted with the responsibility to determine system configurations, create user accounts, assign user permissions, install software updates and patches, set and monitor security settings, etc. Just as accounting departments are monitored by outside auditors for compliance with proper procedures, distributor executives need to provide oversight to systems administrator privileges too.

While the 2015 Data Breach Investigations Report attributed 5.83% of data breaches to insider misuse, the larger threat is from cyber criminals. These threat actors specifically target default administrator passwords and/or weak administrator passwords in order to gain access to company information. Once inside the company network, those with malicious intent often assume the role of system administrator by changing the administrator password. Your company's information can then be held for ransom[2] or stolen outright, havoc wreaked internally, and/or your company used to gain access to another company's networks *(potentially a larger target).*

System Administrator *(aka sysadmin)*

The person responsible for managing and maintaining a multi-user computing environment, including software.

NOTE: A systems administrator's duties include determining system configurations, creating user accounts, assigning user permissions, installing software updates and patches, setting and monitoring security parameters, etc.

CAREFULLY OVERSEE SYSTEM ADMINISTRATOR PRIVILEGES BY ENSURING:

- → *Default administrative passwords are changed during initial installation of all hardware and software.*
- → *Administrative rights are removed from all local devices.*
- → *Administrators have "standard" user accounts for day-to-day business with different passwords.*
- → *Administrators' computers are isolated from your network.*
- → *All Administrators receive data loss prevention training—especially those in non-IT positions.*
- → *System administrators do not access email, the Internet, or documents while signed in to an administrator account.*
- → *Alerts are sent to an appointed executive for all attempts to log-in to administrator accounts.*

A system administrator can make changes affecting system security

Besides changing default administrative passwords on all hardware and software during initial installation, administrative rights should also be removed from all local devices. Administrator accounts should not be used for day-to-day activities such as email or accessing the Internet; instead, administrators should use a "standard" user account with a different password to conduct day-to-day business. If at all possible, the computers administrators use should be isolated from the company network. All administrators—*especially those in non-IT positions*—should receive data loss prevention training. And make sure an appointed executive receives alerts whenever any system administrator attempts to log-in and make changes.

[2] Here's an article about a hospital held hostage by hackers in February 2016 http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html

3 Limit information access to "need to know."

Limiting access to the information a person needs to know to do their job is required to safeguard information from misuse.[3] Otherwise, everyone on the network could access everything on the network—*customer credit card information, company salary information, co-worker's performance evaluations, health care information, financial reports, etc.*

Information security begins and ends with people

Recommended best practice is to develop a framework for access to company information based on job classification, function, and position—*including 3rd party service providers and vendors*—to make sure everyone has access to the information needed for their jobs.

Develop a framework for access to company networks, systems, and information based on job classification, function, and position.

The grid can be as simple as the right to use certain resources *(As shown in the sample below)* or detailed down to the level of authorized connection times, authorized connection locations, and file permissions—*create, read, edit, and/or delete a file.* However, only the designated system administrator is entrusted with determining configurations, installing software updates and patches, setting and monitoring security parameters, etc.

EXAMPLE OF *"NEED TO KNOW"* INFORMATION LIMITATIONS FOR DISTRIBUTOR DIGITAL ASSETS

ACCESS ↓ POSITION →	Warehouse MGR	Branch MGR	Inside Sales MGR	Outside Sales MGR	Credit MGR	Marketing MGR	Purchasing MGR	CEO	CFO	COO	HR MGR	CTO
Cost Information (internal Costs)	🟦	🟨	🟦	🟦	🟦	🟦	🔵	🔵	🟥	🔵	🟦	🟦
Cost Information (supplier Pricing)		🟨	🔵	🔵		🔵	🟥	🟦	🟦	🟦		
Customer Relationship Database	◇	◇	◇	🟥	◇	◇	◇	◇	◇	◇	◇	◇
Employee Information (Healthcare)											🟥	
Employee Information (payroll)	🟦	🟨	🟦	🟦	🟦	🟦	🟦	🔵	🔵	🔵	🟥	🟦
Financial Information (Customer)				🔵	🟥	🔵		🔵	🔵	🔵		
Financial Information (Internal)	🟦	🟨	🟦	🟦	🔵	🟦	🔵	🔵	🟥	🔵	🟦	🟦
Product Information (Internal)	🔵	🔵	🔵	🔵		🟥	🔵	🔵		🔵		🔵
Product Information (Supplier)							🟥	🔵		🔵		🔵
Pricing Database (Customer)			🔵	🟥		🔵		🔵	🔵	🔵		
Pricing Database (Company Purchases)							🟥	🔵	🔵	🔵		
Purchase History (Company)		🟨	🔵	🔵	🔵	🔵	🟥	🔵	🔵	🔵		
Purchase History (Sales to Customer)		🟨	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔵		
Company Website (Infrastructure)	■	■	■	■	■	■	■	■	■	■	■	🟥
Company Website (Content)	▒	▒	▒	▒	▒	🟥	▒	▒	▒	▒	▒	▒
Company-Approved Operating Systems & Software	■	■	■	■	■	■	■	■	■	■	■	🟥

🟦 Access to Department Info   🟨 Access to Branch Info   🔵 Access to Company Info   🟥 Administrator   ◇ View & Record Interactions

■ Use but Cannot Change   ▒ View but cannot change

The framework must be reviewed on a regular basis and continuously updated to reflect changes in roles or employment status—*promotions, demotions, transfers, resignations, and terminations.*

[3] It is also required for PCI Compliance.

METHODICALLY CANCEL ACCESS TO COMPANY SYSTEMS AND INFORMATION 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. Companies without Mobile Device Management (MDM) software need to address removal of company information from personal devices with policy solutions—**employment agreements, confidentiality agreements, use of company information policies, etc.***

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. And the use of Mobile Device Management software enables remote removal of data from mobile devices even if an off-boarded employee changes their password.

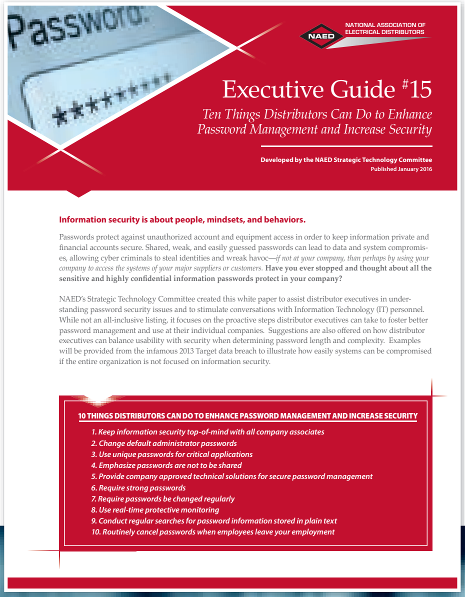
Mobile Device Management, or MDM

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.

4 Require strong, unique passwords.

Passwords protect against unauthorized account 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.*

Password complexity correlates directly with password security



NATIONAL ASSOCIATION OF ELECTRICAL DISTRIBUTORS

NAED

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*

Password complexity is so important NAED's Strategic Technology Committee created a separate document on passwords—***Ten Things Distributors Can Do to Enhance Password Management and Increase Security.***

It offers suggestions on how distributor executives can balance usability with security when determining password length and complexity. Examples from the infamous 2013 Target data breach are provided to illustrate how easy systems can be compromised if the entire organization is not focused on information security.

← **CLICK TO DOWNLOAD EXECUTIVE GUIDE 15**

5 Protect devices accessing networks or storing information with automatic screen lock.

While office equipment, mobile devices, and storage devices contain data you may not want others to access, it's often difficult to remember to log out of applications. Enabling "automatic screen lock" features—*automatically locking the device's screen after a specified time period*—gives a measure of protection should the device be left unsupervised, lost, or stolen. Otherwise, prying eyes could use the device to access information and perhaps even gain unauthorized access to your company's network.

While it may appear unnecessary to "auto lock" the screens of office equipment located on company property, the 2015 Data Breach Investigations Report disclosed 5% of data breaches would have been prevented if the "auto screen lock" feature had been enabled in the office.

Enabling "Automatic Screen Lock" prevents data breaches

The more sensitive the information a device is accessing, the quicker the device's screen should automatically lock. For example, access to bank accounts and personally identifiable information should be locked immediately at the end of a session. On the other hand, the length of inactivity in the general office area could be as long as 15 minutes. Solutions for distributor counter areas will vary by company; some use digital cards to facilitate immediate account log-in and log-out efficiently.

SUGGESTED AMOUNT OF INACTIVITY BEFORE "AUTO SCREEN LOCK" IS ENABLED

- **Bank Accounts:** *Lock screen immediately (30 seconds of inactivity)*
- **Personally Identifiable information in HR:** *Lock screen immediately (30 seconds of inactivity)*
- **Credit and Accounting:** *Lock screen after 5 minutes of inactivity*
- **General Office:** *Lock screen after 15 minutes of inactivity*
- **Counter area:** *Distributor preferences for locking screens may vary from immediately to 5 minutes*

Screens with more sensitive information should automatically lock quicker

6 Use passcodes to "unlock" screens and devices.

After "auto lock" is in place, users will be required to enter passcodes to "unlock" the device's screens. Recommended best practice is for devices to be automatically locked out for at least 30 minutes after 5 unsuccessful log-in attempts—*i.e., the wrong passcode is entered*—within a 30 minutes time frame.

Each company should develop methods to automatically handle unsuccessful log-in attempts before intervention is required by the system administrator. The key is to differentiate between employees who forget their passcode and someone with malicious intent trying to use a lost or stolen device.

Employees who forget their passcodes can gain access to their device automatically by identifying themselves through a second means of identification. Alternately, information on lost or stolen devices can be erased remotely with Mobile Device Management software.[4]

Automatically lock out devices after 5 unsuccessful log-in attempts within 30 minutes

7 Offer company approved data storage and disposal solutions.

Every time electrical distributors receive, store and/or transmit information there is risk of a data breach. According to the 2015 Data Breach Investigations Report, 10.6% of data breaches were the result of associates abusing the access they have been entrusted for either financial gain or using an unapproved work around to speed things up to make their job easier. Cisco Systems also reports a rapid rise in unauthorized usage of cloud storage by company associates.[5]

Distributor executives can mitigate these risks by providing company approved data storage and equipment disposal solutions to associates. Otherwise, company associates will come up with their own solutions —*unsecure CDs, USB "flash" drives, preferred personal "cloud" storage systems, etc.*—to transfer information to other computing devices. Data breaches can then occur due to insider misuse, device theft or loss, or unapproved device disposal.

EXAMPLES OF WAYS TO STORE OR TRANSFER INFORMATION

- **"Cloud" storage sites**
- **Mobile equipment memory:** *Laptops, smartphones, tablets, etc.*
- **Office equipment memory:** *Copiers, desktop computers, printers, etc.*
- **Print the information:** *Produce "hard copies"*
- **Servers**
- **USB Flash Drives**
- **Back-up disks & CDs**

[4] Mobile Device Management software typically "wipes" the mobile device after 10 unsuccessful log-in attempts in a row.
[5] "Cisco Reports Rapid Rise in Unauthorized Cloud Usage, "Wall Street Journal, January 13, 2016 http://www.wsj.com/articles/cisco-reports-rapid-rise-of-unauthorized-cloud-usage-1452690000

If company approved data storage and equipment disposal solutions are not available, associates will come up with their own solutions

Your company's information security policy should specify company approved storage and disposal solutions—*including cloud storage*[6] *and portable storage devices*—and include a process for immediately reporting lost, stolen, and compromised devices. If your company opts to allow portable storage devices, make sure password protection and data encryption are required and enabled. Also consider limiting CD and DVD drives to read only memory (ROM).

If allowed, USB drives should be password-protected and the data encrypted

If your company elects to use cloud storage, make sure it integrates seamlessly with the backup and file storage systems used for desktop computers, mobile devices, servers, etc. Microsoft Office 365, Dropbox, OneDrive for Business, and Box are examples of cloud-based storage tools electrical distributors can use to access, share and edit documents and files anywhere, anytime.

SECURE INFORMATION DISPOSAL

Special care must be made to remove corporate data when a device is replaced---whether company or associate-owned. Minimize the risk of data recovery by those with malicious intent by making it impossible for anyone to retrieve data after disposal—reformat, "wipe" the device clean, or physically destroy drives, flash cards, etc.

All printed information containing confidential and personally identifiable information (PII) should also be disposed of securely to minimize the risk of the printed information falling into the wrong hands.

[6] The security of information stored "in the cloud" depends on the security measures the cloud provider takes to ensure your data is protected.

8 Provide secure wireless connections for remote users.

Remote access to company networks through unsecure public Wi-Fi connections—*airports, hotels, restaurants, etc.*—and associates' home Internet connections makes it easy for information to fall into the wrong hands. Therefore, electrical distributors must develop a mobile device security policy[7] and deploy mobile device management (MDM) solutions to protect their data from possible breaches.

Offer Secure Options for Anywhere Connectivity

Virtual Private Network, or VPN

A technology creating an encrypted connection over a less secure network.

The most common means of gaining remote access to company information and resources are via Virtual Private Networks (VPNs).[8] VPNs allow secure remote access to a company's network resources by establishing an encrypted connection across the Internet.

Some of the benefits of VPNs include the ability to assign and administer access rights tailored to individual users, such as employees, contractors, or partners; enhanced productivity through extension of corporate networks and applications; reduction of communications costs; as well as greater flexibility in office space and site planning.

VPNs can create significant exposure to risk from incoming connections and devices, it is ESSENTIAL that any devices connecting over a VPN have up-to-date antivirus protection, and that the VPN Gateway itself has an integrated firewall, antivirus, anti-spyware, and intrusion prevention—*or is connected to a firewall with intrusion prevention.*

PROVIDING INTERNET ACCESS FOR COMPANY "GUESTS"

Many electrical distributors provide "guest" Internet access as a complimentary service for customers and visitors.

If your company chooses to provide such a service, be sure to require agreement with your Terms of Use before allowing internet access, completely isolate the "guest" access from company networks and systems, and monitor guest access to make sure it is not abused or illegal information downloaded.

[7] For additional information, please refer to Executive Guide 5: Mobile Device Security Policy http://www.naed.org/NAEDDocs/Research/Benchmarking/Mobile_Device_Security_Policy.pdf

[8] An alternative secure connection option is a Virtual Desktop Infrastructure (VDI). VDIs allow users to access hosted applications and documents via the Cloud using any internet connection.

9 Use at least two ways to authenticate Systems Administrators and remote users.

Strong passwords aren't enough protection from cyber criminals for two types of users—*systems administrators and remote users.*[9] The 2015 DBIR reported 24% of data breaches could have been prevented through the use of two-factor authentication to ensure only the authorized user is accessing company networks and information.

Two-Factor Authentication, or 2FA

Using two different means of verifying a user is who they claim to be. The first method is generally a password. The second method is often a user-created response to a security question or requires a previously registered physical device be used for verification.

While there are concerns about the inconvenience of two-factor authentication for remote users, simple and effective two factor authentication systems can be implemented by electrical distributors. For example, users of popular websites including Amazon®, Google®, and Microsoft Outlook® are required to use two means to verify their identity the first time they log on with a new device—*their password and a second factor delivered via their preferred method of phone or text.* An email disclosing the log-in from the new device is also generated and mailed to their preferred email account. Subsequent log-ins from the same device only requires a password, unless the device is used infrequently.

Two-Factor Authentication protects against hackers using stolen passwords to log-in to company networks

Besides PINs delivered via phone or text, secondary methods of user authentication include hardware or software tokens, mobile apps, one-time passwords, security pictures, security questions, smart cards, certificates, USB security keys, etc. Other, more sophisticated identification methods are also available including biometrics—*fingerprints, voice recognition, facial recognition, iris scanning, etc.*

TWO-FACTOR AUTHENTICATION (2FA)

FIRST FACTOR	+	SECOND FACTOR
PASSWORD	**+**	**ADDITIONAL MEANS OF CONFIRMING USER'S IDENTITY**
		Something the user has: • *PINs delivered via phone or text* • *Hardware or software token* • *Mobile apps* • *One-time passwords (OTP)* • *Security pictures* • *Security questions* • *Smart Card* • *Certificate* • *USB security key* **— OR —** ***Something the user is:*** • *Biometrics*

[9] In addition, PCI-DSS 8.3 requires two-factor authentication for remote access to the network by employees, administrators, and third parties.

10 Make sure information security basics are covered too.

"Walk the talk" by sitting down with your IT personnel to gain an understanding of all the mechanisms your company has in place to prevent and detect data breaches. Suggested agenda items include how browsers and software are kept current; how anti-virus software, firewalls, and network segmentation are used to protect company information; how your company's website is protected; how company data is backed up; how emails are filtered to prevent "phishing;" how access to certain websites and apps is restricted; how user behavior such as information usage and downloads are monitored; and how the 3rd party security audits of company systems are conducted. Then develop and communicate straight forward company information security policies. And make sure to reinforce the importance of adhering to the company information security policies with ongoing training.

Recommended Resources

Center for Internet Security®

The CIS Critical Security Controls for Effective Cyber Defense
https://www.cisecurity.org/critical-controls.cfm

Kaspersky Lab

Small Business IT Security Practical Guide
http://media.kaspersky.com/en/kaspersky-small-business-it-security-practical-guide.pdf

NAED's Strategic Technology Committee

Executive Guide #8: IT Disaster Recovery Planning
http://www.naed.org/NAEDDocs/Research/Benchmarking/IT_Disaster_Recovery.pdf

Executive Guide #14: Information Security is Everybody's Business
http://www.naed.org/NAEDDocs/Resources/Business%20Tools/Technology/Executive_Guide_14_Information_Security.pdf

Executive Guide #15: Ten Things Distributors Can Do to Enhance Password Management and Increase Security
http://www.naed.org/NAEDDocs/Resources/Business%20Tools/Technology/ExecGuide15_TenThings.pdf

Password Management Infographic
http://www.naed.org/NAEDDocs/Resources/Business%20Tools/Technology/10ThingsToIncreaseSecurity.pdf

What You Can Do

A few things can make a big difference in the security of your company's information. Here are four strategic actions electrical distributor executives can take to prevent the loss of data:

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.

Additional tools from NAED's Strategic Technology Committee are available for download at www.naed.org/strategictechnology.