NATIONAL ASSOCIATION OF ELECTRICAL DISTRIBUTORS

Executive Guide #14

Information Security is Everybody's Business

Developed by the NAED Strategic Technology Committee

Published August 2015

INTRODUCTION

Almost every day, there is another headline about a major data breach at a well-known company. Managing the constant stream of information security vulnerabilities is the new normal for executives, regardless of industry, revenue, or number of employees. If giants of industry and government agencies can be hacked, how can electrical distributors protect themselves from unauthorized data breaches and intrusions?

Ensuring data security across all locations and devices has ranked as a top technology concern by more than 96% of distributor executives responding to the NAED Technology Benchmarking Survey for each of the past four years. Therefore, NAED's Strategic Technology Committee created this white paper, ***"Executive Guide #14: Information Security is Everybody's Business,"*** to assist distributor executives in understanding the business risks of information security and to provide insight into what distributor executives can do to mitigate information security risks.

Information security is…

1. A risk of doing business;
2. About people, mindsets and behaviors; and
3. An ever-evolving threat.

WHY INFORMATION SECURITY IS IMPORTANT TO ELECTRICAL DISTRIBUTORS

1. Information security is more than just a technology issue. It is an ongoing risk of doing business. Every time electrical distributors receive, store and/or transmit information there is risk of a data breach. Any party your company "connects" to—*customers, vendors, third party service providers and any other party your company exchanges information with*—also needs to be diligent about information security.

Exhibit 1 lists the top information security threats from the 2015 Data Breach Investigations Report[1], which collects information from 70 global information security organizations.[2]

Exhibit 1. Top Information Security Threats
Source: 2015 Data Breach Investigation Report

28.5%	**POS Intrusions** - Remote attacks to obtain credit card information.
18.8%	**Crimeware** - Malware to gain control of systems as a platform for illicit uses—stealing credentials, Denial of Service attacks, etc.
18.0%	**Cyber Espionage** - Unauthorized network access with the motive of spying using malware.
10.6%	**Insider Misuse** - Unapproved or malicious use of organizational information.
9.4%	**Web App Attacks** - Exploiting web applications for vulnerabilities or using stolen credentials to impersonate a valid user.
8.1%	**Miscellaneous Errors** - Mis-delivery of information and unintentional actions (except lost devices) compromising information security.
3.3%	**Physical Theft/Loss** - Misplacement of computers, laptops, cell phones,drives and/or documents or information copied for unauthorized use.
3.1%	**Payment Card Skimmers** - Installation of a device on credit card devices equipment to read and intercept magnetic stripe data on payment cards.
0.1%	**Denial of Service (DoS)** - Attacks compromising networks, applications and systems.

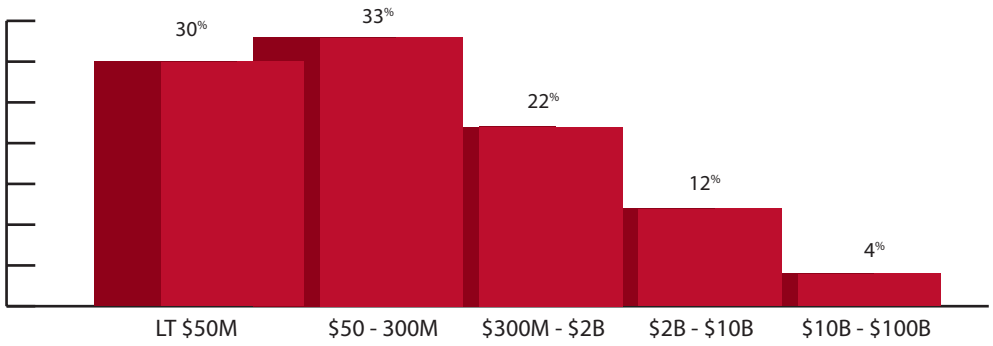
[1] Download the 2015 Data Breach Investigations Report
NOTE: While this report was compiled by Verizon, it analyzes data breach information from all Internet Service Providers (ISPs) that was collected from 70 global information security organizations.

[2] Examples of entities contributing information to the 2015 Data Breach Investigations Report include the U.S. Computer Emergency Readiness Team (US-CERT), the U.S. Secret Service, the Council on Cyber Security, forensic providers and information security product and service providers including FireEye, Fortinet, Kaspersky Lab, McAfee, Palo Alto Networks, Wombat Security Technologies, etc.

Data breaches at smaller companies seldom make headlines

Think your company is too small to be at risk for a data breach? Think again. Information security breaches at larger, more well-known companies may make the headlines, however, a study of insurance claims from 2011-2013 shows smaller companies are more often the targets because their systems are often not protected as well (See Exhibit 2). For example, the cyber criminals involved in the Target data breach gained entry to Target's information systems by using the credentials of a small, local HVAC vendor's invoicing system.

Exhibit 2. NetDiligence® 2014 Cyber Claims Study
Security Breaches by Company Size
Based on Cyber Liability Insurance Claims 2011-2013



Distributor executives must ensure their company is taking prudent steps to protect 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 your operations; result in lost sales; damage company reputation and brand; and lead to significant out-of-pocket costs.

Home Depot's 2014 Annual Report refers to "at least 57 civil lawsuits to date" related to its data breach and a study of insurance claims from 2011 – 2013 by NetDilligence® reported an average claim payout for data breaches of $733,109.[3]

While it is extremely difficult to quantify damage to reputation and brand, information excerpted from The 2015 Data Breach Investigations Report is provided in Exhibit 2 to help distributor executives gauge the magnitude of their individual company's out-of-pocket cost exposure. Keep in mind failure to take a proactive approach to information security exponentially increases a company's risks (and associated costs) for information security breaches.

[3] Not all commercial general liability insurance policies cover data breaches.

Exhibit 3. Estimated Out-of-Pocket Cost of a Data Breach Based on the Number of Records Lost
Source: Adapted from information in the 2015 Data Breach Investigations Report

# Records Lost	Expected Cost of Breach
100	**$25,450**
1,000	$67,480
10,000	$178,960
100,000	$474,600
1,000,000	$1,258,670
10,000,000	$3,338,020
100,000,000	$8,852,540

"For a company that isn't prepared, a breach can quickly become a crisis that spirals out of control. Mistakes made in the first 72 hours can result in greater direct financial losses and a badly tarnished reputation that lasts for years." -Advisen Insurance Intelligence ©

Electrical distributors who prepare for a data breach in advance can minimize reputational damage, costs associated with responding to the data breach and third party lawsuits. The first step for executives in understanding the precautions your company needs to take is understanding where your company is today.

Do you know…

- What data your company needs to protect?
- What mechanisms your company has in place to prevent and detect data breaches?
- What your company's information security vulnerabilities are?
- What proactive steps your company is taking to address the consequences of any possible information security event?[4]
- How data breaches are covered by your commercial general liability insurance?

[4] NAED has developed several business tools for electrical distributors to help with business continuity issues, including a disaster planning website and Executive Guide #8: IT Disaster Recovery.

"We have met the enemy and he is us." -Pogo (Walt Kelly)

2. Information security begins and ends with people. Associates whose information security awareness is lacking or out-of-date leads to careless behaviors—*working around security tools, responding to fake requests for password resets, clicking on malicious links, or opening the fake attachments*—which cyber criminals rely on to install malware or exploit security gaps. (See Exhibit 4).

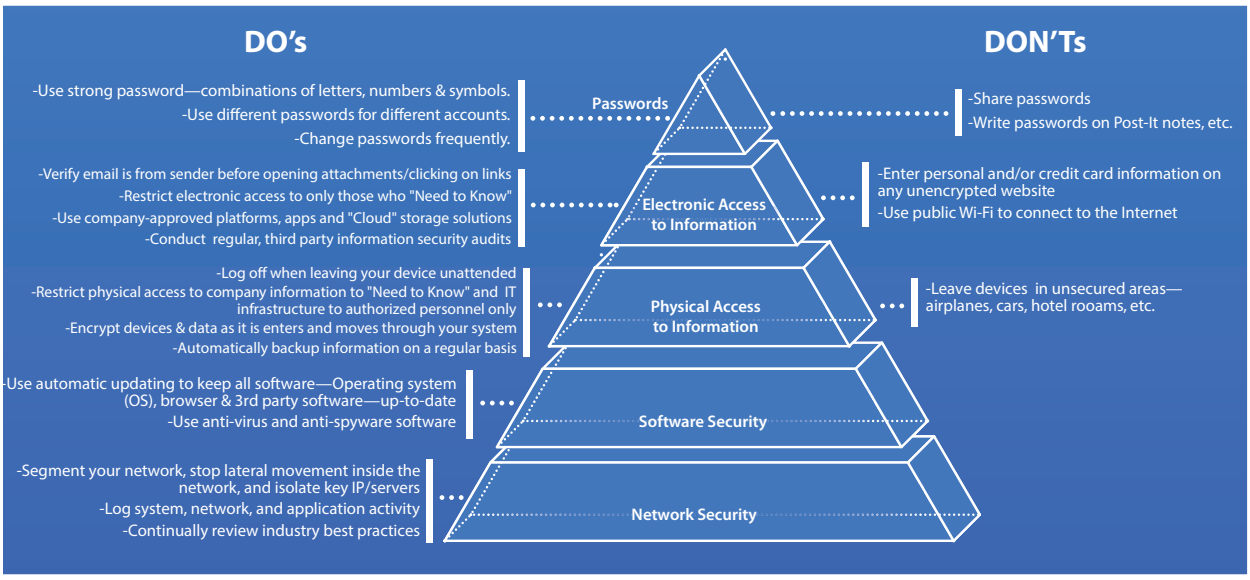
More than 80% of data breaches are directly linked to people

Exhibit 4. Impact of Associates on Information Security
Source: 2015 Data Breach Investigations Report

Top Information Security Threats		How Associates Can Enable Data Breaches
28.5%	POS Intrusions	"Phishing" campaigns often used to obtain Passwords
18.8%	Crimeware	39.9% Malware installed via email attachment 37.4% Malware installed via email link
18.0%	Cyber Espionage	
10.6%	Insider Misuse	55% Privilege abuse: Employees abusing the access they have been entrusted with by their organization for either financial gain ***OR*** using an unapproved work around to speed things up or make their jobs easier.
9.4%	Web App Attacks	
8.1%	Miscellaneous Errors	30% Sensitive information reaching the wrong recipients 17% Publishing nonpublic information to public web servers 12% Insecure disposal of personal data
3.3%	Physical Theft/Loss	55% of thefts occurred within the victim's work area 22% of thefts occurred in employee-owned vehicles
3.1%	Payment Card Skimmers	
0.1%	Denial of Service	

However, associates who have a clear understanding of and commitment to information security; receive ongoing education and training about the latest information security; practice safe computing behaviors (See Exhibit 5); are on the alert about possible means of intrusion; and know what to do if they spot suspicious activities are an electrical distributor's best defense against data breaches.

Exhibit 5. Safe Computing Behaviors



Distributor executives ensure: straight-forward information security policies are developed and communicated; reinforce the importance of information security with ongoing training—*available in NAED's VIP Access Core Library*[5] *or from companies such as Wombat Security Technologies*—and conduct vulnerability assessments.

Do you know…

- What information security awareness training your associates receive on an ongoing basis?
- How your company assesses and reinforces safe computing behaviors in the normal course of day-to-day operations?

3. Electrical distributors' information systems are vulnerable to an increasing threat of continually evolving cyber security risks. Cyber criminals are developing more and more sophisticated ways to exploit information security vulnerabilities by constantly probing for any weaknesses in networks, software and people.

The need for innovative solutions to prevent data breaches has led The Occupational Outlook Handbook to project information security analyst job growth of 37—*much faster than average*—through 2022. Merrill Lynch recently created a new, unique segment to the information security market—*Advance Threat Protection*—and reports a 64% growth rate year to year.[6]

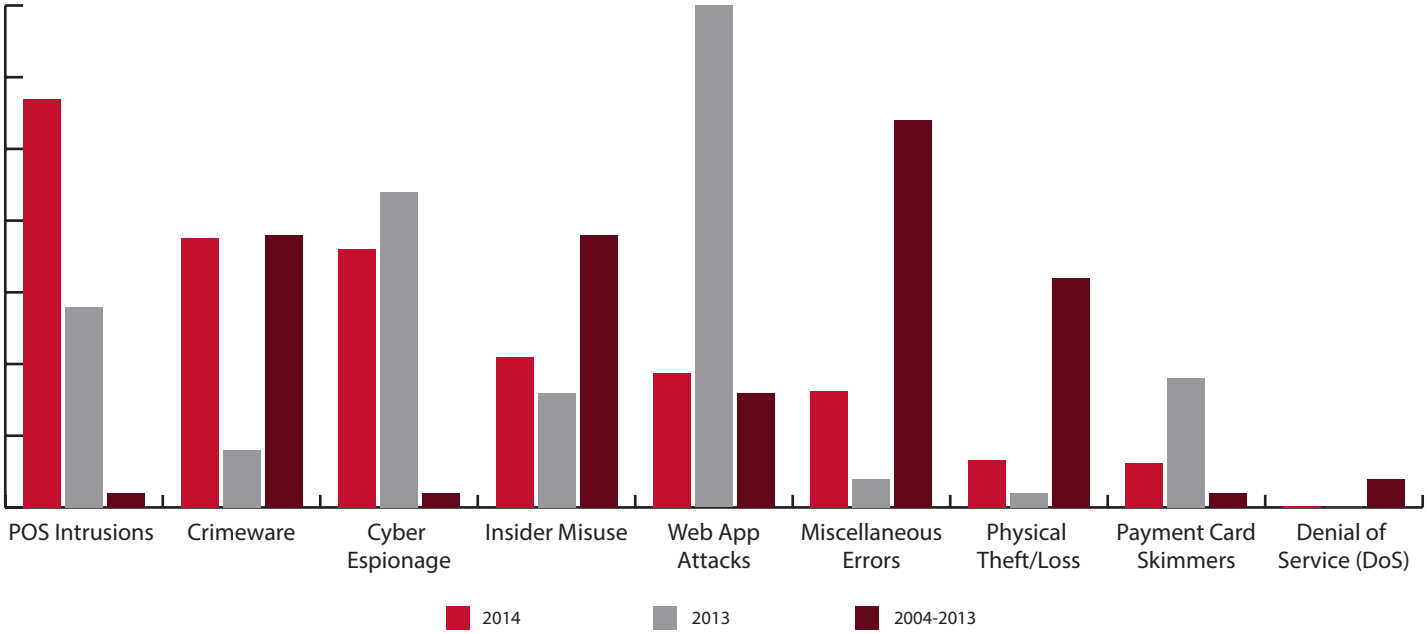
Cyber criminals are getting more adept at evading detection in networks by changing tactics from moment to moment, disappearing from a network when they are detected and then rapidly using

[5] Information courses in NAED's VIP Access Core library include Introduction to Information Security, Using your Desktop Computer and Mobile Devices Safely and Using E-mail, the Internet and Social Media Safely in a Corporate Environment.

[6] Merrill Lynch's The RIC Report, July 14, 2015

another method to gain entry. Other cyber criminals exhibit patience and blend in, taking time to establish multiple footholds before taking action. However, while the tactics cyber criminals are using are becoming more and more sophisticated, the top nine information security threats have remained the same over the last 11 years (See Exhibit 6).

Exhibit 6. Changing Information Security Threats
Source: 2015 Data Breach Investigations Report



Cyber criminals are also exploiting software vulnerabilities, with more than 99.9% of exploited vulnerabilities having patches available for more than a year.[7] And more sophisticated non-technical attempts are being made to gain access to company information—*often referred to as social engineering*—by tricking users into resetting passwords, installing malware, or unwittingly helping exploit security gaps in out-of-date software.

As for information security beginning and ending with people…accidental or intentional information leaks, unauthorized information use and sabotage of the company systems in return for a perceived slight are information security risks for electrical distributors too.

[7] 2015 Data Breach Investigations Report

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; and
4. Conduct ongoing, regular 3rd party security audits to identify your information security vulnerabilities.

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 TOPICS INCLUDE:

- Physical Access
- Electronic Access
- Software Security
- Network Security