PRICE CHECK:

COULD YOUR RETAIL STORE BOUNCE BACK FROM A LOSS?

2018 CHALLENGES FOR SMALL RETAIL BUSINESSES

Table of Contents

INTRODUCTION

As department and big box stores struggle to reinvent themselves in the shadow of online goliaths, small retail businesses seek their place in a shifting landscape being redefined by consumers' ever-expanding digital appetite. Online shopping continues to grow, and those shoppers increasingly are turning to their smartphones for purchases, with 48 percent of mobile users surveyed saying they've bought an item on their phone, according to the 2017 UPS Pulse of the Online Shopper study.[1] That's a seven-point increase in just two years. Further, the survey shows that roughly 80 percent went online to do research or to purchase the product, meaning only about 20 percent of their purchases were defined in traditional terms of a customer walking into a store and buying a product outright.

Savvy shop owners know they must embrace the digital desires of their potential customers and weave in-store experiences together with mobile and web versions, as a smart Facebook post can generate interest about a special in-store sale and a clever mobile strategy can reinforce the face-to-face relationship with clients. Forward-looking retailers also know they can use data on customer interests to enhance store encounters and build loyalty programs.

But a growing digital retail space brings with it emerging risks for the small retailer. More than ever, it's important to take the right precautions when it comes to customer data and transactions to keep them secure. With preparation, you can protect your business in a data-driven world, while also helping to best position your operation against unforeseen circumstances that could affect your store, your employees or your assets, or interrupt your ability to serve customers. In today's competitive retail environment, that's where your focus needs to be — your customers.

CHANGING SHOPPING PATTERNS

80% Went online during their search or purchase phase

20% Went to a store to select and purchase

Citations and links can be found in the citation summary ›

PART I: YOUR CUSTOMER DATA

EMERGING EXPOSURES IN A DIGITAL WORLD

But I'm Not a Target! No Hacker Would Come After Me.

Wrong. Hackers are not selective when it comes to their victims. The headlines about data breaches may be dominated by scandals that have hit major chains such as Home Depot, but if you have data that hackers can access and sell, you can be a target.[2] For example, a small neighborhood grill in Seattle was ensnared by an international identity theft ring. Thieves hacked into its retail point-of-sale system and stole customer credit card numbers. The Russian cybercriminal at the center of the operation was tracked down on vacation in the Maldives, tried in the U.S. and sentenced to 27 years in prison,[3] but the grill did not recover.

In fact, the Identity Theft Resource Center's annual data breach report features page after page detailing malware attacks, phishing scams and other cybercrimes striking all types — and sizes — of businesses.[4] A malware attack on an outdoor sporting goods store in Oregon enabled cybercriminals to gain access to customer payment information for more than a month before they were discovered and neutralized. Similarly, the owners of a clothing store in Florida noticed suspicious activity and reported their e-commerce server was compromised. Forensic investigators discovered customer credit card information was illegally accessed for almost a week. The store's owner had to send the letter no retailer wants to send to customers, detailing how their personal credit card information may be in the hands of criminals after a visit to her store.

"The bad guys — they are looking for companies big and small, and sometimes they will specifically go after small companies because they know their security is likely not as robust, that their employees may not be as wary of these types of attacks," says Nick Graf, Consulting Director of Information Security for CNA, Risk Control. "Sometimes they'll go after a small company and use that to perfect their skills. If something goes wrong, it's no big deal; this is just a small target anyway."

THE PRICE TAG: What's the Potential Cost of a Cyberattack?

Data Breaches by the Numbers

$7,115.26

Average cost to a small business, according to the National Small Business Association.[5]

42% of small business owners reported having been hacked.[6]

1/3 of consumers say they will shop elsewhere if their retailer of choice is breached, according to a study by Javelin Strategy & Research.[7]

Cleanup following an attack can involve the hiring of forensic investigators, legal counsel and public relations professionals as well as costs related to notification of customers, free credit monitoring and other services offered to the victims.

Citations and links can be found in the citation summary ❯

Secure Swiping: Credit Card Safety for Retailers

Most small retailers outsource the credit card payment process to a third party, which sometimes can provide a false sense of security as retailers believe they have handed over the responsibility and the worry to the external partner. "The problem with that is that it's unfortunately not true," Graf says. "Yes, you've outsourced it, and yes, there probably is some liability shift that has occurred, but it's definitely not 100 percent."

Take the experience of Jimmy John's sandwich shops, which saw more than 200 stores hit by a data breach. Cyberthieves accessed store point-of-sale systems via a username and password that the third-party payment processor used to manage devices remotely. They installed malware designed to steal customer credit card information off the devices.[8] In this case, Jimmy John's was not the one to allow access to the information, but "all the headlines were 'Jimmy John's suffers massive credit card breach,'" Graf says. "In reality, Jimmy John's itself didn't actually suffer that breach but it had a third-party payment processor who had set up to administrate all of its credit card systems and unfortunately didn't do it properly." Jimmy John's stores still had to deal with the public relations fallout from the breach, which included the filing of a class action lawsuit.[9]

To fortify your customer data systems, think through all the points in your system where transactional data may live. When setting up a credit card system, verify that the payment processor is handling sensitive customer information correctly. They should make sure the company is properly credentialed by the Payment Card Industry (PCI) Security Standards Council and meets its Data Security Standard (DSS).

The PCI Data Security Standard (PCI DSS) requires secure networks, cardholder data protection and encrypted transmissions, among other things.[10] Retailers should make sure not only that their payment processor is PCI certified but that the processing system, which is the hardware that could be the point-of-sale system in your store where the credit card swipe takes place, is PCI DSS validated. "Ask if the systems were installed by a Qualified Integrator and Reseller," Graf says.

The best course of action for retailers with a third-party payment processor is to not store, transmit or process any PCI data, Graf says. From the point of the credit card swipe or dip, the data should be transmitted directly to the payment processor, never touching the retailer's network. Retailers should look for a PCI-validated, point-to-point encrypted solution, according to Graf, as encryption converts the data into an unreadable form.

Citations and links can be found in the citation summary ❯

DATA DICTIONARY[11]

PCI Compliance = Credit card processors are "PCI compliant" if they meet the standards of the Payment Card Industry (PCI) Security Standards Council, a global organization founded by the major credit card companies. PCI has created the PCI Data Security Standard to help safeguard payment data.

QIR = Qualified Integrator and Reseller is someone who is trained for secure installation of payment applications to help comply with the PCI Data Security Standard.

Point-to-Point Encryption = Combines secure devices, applications and processes that encrypt data from the point of interaction at your store (such as the swipe or dip) until the data reaches a secure decryption environment.

Data Defense: How to Protect Your Customer Info

To protect your data, train your employees to avoid the human errors that were to blame for 34 percent of CNA cyber claims from 2012-2016. Human error may include mistakes such as misdirected emails, misconfigured hardware or a scam that succeeds in soliciting information from an authorized user. Security awareness training for yourself and your employees can help prevent an unsuspecting and overly trusting employee from clicking on something that puts your entire network at risk. Employees also should be instructed never to give personal information to cold-callers or to enter information in response to unsolicited emails.

"Social engineering" is a technique used by cybercriminals to trick or manipulate authorized users to turn over sensitive information that is then used to access systems, or to install malware. These plots may come in the form of an email containing a fake message from a company CEO asking employees to turn over personal information or passwords. The messages may look legitimate, and include duplicated logos and names. Sometimes they aim to create a sense of urgency by warning something bad will happen if the person doesn't act, such as losing access to an account.

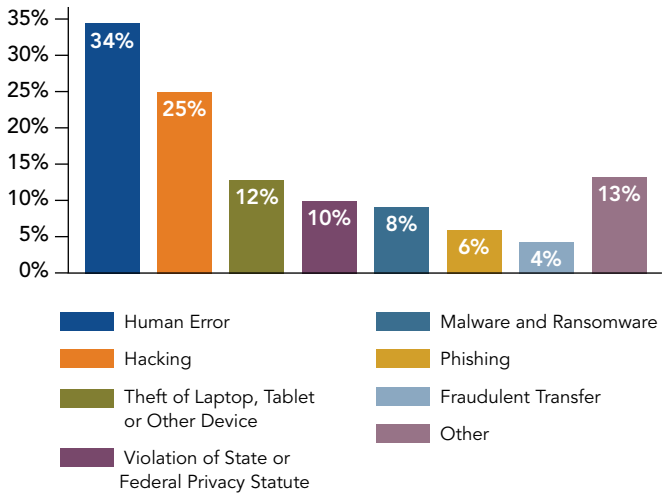
While often these scams arrive in email form, they also can come by phone and even through in-person scams. Thieves may call and pretend to represent your payment processor and try to pull important sign-in information from an employee.

Hacking incidents, which involve thieves exploiting vulnerabilities in servers and firewalls to access information without permission, accounted for 25 percent of CNA's cyber claims, second only to human error. The theft of a laptop, tablet or device also came in near the top, and was responsible for 12 percent of claims.

"Devices will inevitably be lost, and, if they're not utilizing full disk encryption, that almost always becomes a breach notification scenario," in which laws are triggered requiring customers be notified, Graf says. There may be no proof that the device's data was used by criminals, as the thieves may have stolen the laptop solely for the value of the device, without awareness of the sensitive data it contained. However, the mere fact that the laptop landed in unauthorized hands may still trigger data breach notification laws, "because custody of that information is lost," Graf says. "That situation can turn a thousand dollar laptop loss easily into a six- or seven-figure claim very, very quickly."

Be sure to use strong passwords on your systems and devices and change them often. Restrict access to only the most essential employees. Retailers should employ multifactor authentication, or

Cyber Claim Frequency Analysis[12]



CNA Claim Data 2012 – 2016. All Segments – Closed Claims.

The information used to compile the data and the corresponding chart includes claims that may fall into more than one category. Accordingly, the resulting percentages may not total 100 percent.

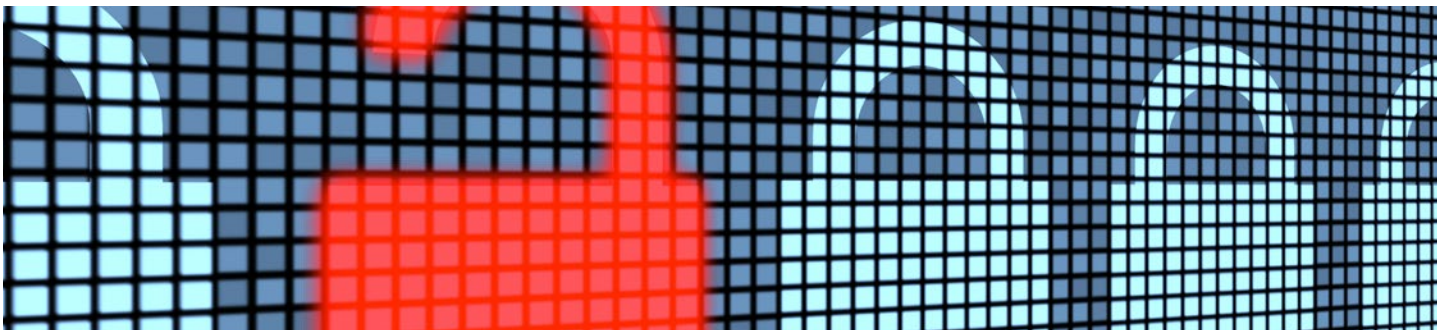
Human error is to blame for **34 percent** of **CNA cyber claims** ...

two-factor authentication, to provide added security on devices used for remote access or when accessing cloud-based resources. Multifactor authentication means two pieces of information are required in order for a user to gain access, which could involve a combination of a password, a regularly changing code sent to your phone or a fingerprint reader. "Many cloud-based service providers offer the option of two-factor authentication; it's just typically not required. It's something optional the customer would need to go in and enable for their account, but again offers a huge increase in security compared to not having it," Graf says.

Ransomware attacks continue to pose a threat and can hit companies large and small. "The bad guys with ransomware—they don't care who you are," Graf says. "They use malware, they encrypt your data, locking you out of it and they demand a ransom or a payment of at least a few hundred dollars to unlock that data."

Hit by Hackers? Now Tell Your Customers

Almost all states have data breach notification laws, which vary in requirements but necessitate that businesses alert customers of unauthorized disclosures of their personal information. When a data breach occurs, you must comply with the laws of the states where the affected customers live, which can make it tricky to navigate the legal requirements. "It doesn't matter where the data was located and it doesn't matter where the laptop was lost," Graf says. "It really matters where all those individual affected customers live." If you had a breach that resulted in thieves accessing information from customers in Connecticut, Illinois, Virginia and New York, who made purchases at your store, you would have to comply with the laws in each of those states. "It can be very difficult, all of a sudden, to be sure you're complying with all these different laws, so you will not have state attorney generals breathing down your neck asking why you're not protecting their constituents," Graf says.



WHAT TO DO POST-BREACH[13]

If you do not have the necessary skills in-house to deal with a cyberattack, line up vendors who do. If an attack occurs, here are some tips from the U.S. Department of Justice's Cybersecurity Unit:

- If an attack happens, "image" the affected computers, which may require law enforcement or expert assistance, but you should try to document everything you can about the attack.
- Halt ongoing damage to the system. This may mean rerouting network traffic or isolating all, or parts, of the compromised network, among other steps.
- Notify relevant personnel within your organization, as well as law enforcement, if appropriate. Determine if the breach has triggered notification laws requiring you to inform customers that their information may have been compromised.
- Do not use the attacked system to communicate.
- Remain vigilant for repeat attacks.

Citations and links can be found in the citation summary ❯

I Have Chip Technology, Does It Protect Me?

"Chip technology is a great step in the right direction, but chip by itself is not a silver bullet," Graf says. Data breaches still occur even with upgraded chip credit card technology. As Graf explains, chip technology protects against the physical creation of fraudulent credit cards. With a traditional magnetic stripe credit card, if thieves obtained your information, they could buy an inexpensive magnetic reader, plug it into a computer and write magnetic data onto a blank credit card to duplicate your physical credit card. With chip technology, data is stored on the card chip, which is difficult to duplicate, so it protects against forged credit cards being created from stolen data. However, the chip does not protect against card-not-present transactions, which occur via online purchases. "Chip protects against certain things but just because you accept chip transactions, it doesn't automatically mean that information is encrypted as it flows through your network back to the payment processor," Graf says. "A separate technology called point-to-point encryption, also referred to as P2P encryption, is required for data protection."

The Backup Plan

Data backup is essential and should be part of your store's daily routine. While there is potential for valuable data stored on your computers to be stolen by hackers remotely, it also can be lost through more traditional ways, if your computer equipment is lost, stolen or damaged.

Small retailers who want to protect themselves in case of a lost or stolen laptop should opt for full disk encryption. "Thankfully most modern operating systems, (Windows 10 Pro, Mac OS X, iOS iPhone, and Android), all support full disk encryption natively, meaning no additional software needs to be purchased. In most cases, it simply requires enabling the encryption functionality," Graf says.

Experts also recommend taking steps to protect your computer systems from power surges, which can fry your equipment. "Any small business in the retail space can work with their utility company to have affordable surge protection set up," says Marjorie Gates, CNA's Risk Control Consultant overseeing Small Business. In addition to making routine data backups a regular step in your day, make sure you are testing for the restorability of your data. Retailers may believe they have robust data backup strategies in place, and follow a certain protocol for years, thinking they are safe. Only when a disaster hits do they discover that there was a glitch in their system and data can't be restored. "Testing that restorability is also very important these days, especially for small businesses," Graf says. A cloud-based backup solution might be a good option as well, because it's off-site and a secure, third-party location.

What If I'm Still Using Paper?

You wouldn't be alone. When it comes to keeping inventory, roughly 1 in 7 small businesses surveyed still rely on a manual process such as pen and paper. A similar number also admit to using pen and paper when it comes to keeping track of assets as well, according to the 2017 State of Small Business report.[14]

If a fire or water damage event occurs, those crucial records can be lost. A fire-resistant safe is helpful, but can give a false sense of security, says Gates. "If they have a really big fire, what we see time and time again is that the room gets so hot, and the fire-resistant safe gets so hot, that the documents inside incinerate anyway, even if they haven't been touched by flames, because everything's so hot," she says. She recommends you make copies, and create a backup by storing copies offsite so you don't lose your contracts or the information that enables you to send out regular invoices. "Try never to have anything that is singular and important just in one place," she says.

INSURANCE CONSIDERATIONS

CYBER INSURANCE. Insurance needs for physical building space may be obvious, but cyber may be a new area for retailers to consider when planning insurance coverage. Such insurance usually covers the costs involved in recovering from a data breach, such as customer notification and monitoring services. Even if you've taken steps to secure your network, hackers remain determined to find new ways to steal valuable data. Evaluate your insurance policies to make sure you have the right coverage in the case of a data breach event.

BUSINESS INCOME. A data breach can hit like a storm, interrupting your business and causing a shutdown, which can lead to loss of customers and income. Business income coverage reimburses net income and operating expenses lost during the period following a loss. Negative headlines about stolen credit card information could erase the hard work you've invested in customer relationships. Business income insurance can help keep a retailer in business until it can get those customers back in the door. Some insurers might offer or include "extra expense" coverage in case you need to open in a new location as soon as possible.

TAKEAWAYS

- **Train your staff** how to recognize potential cyberscams and avoid being duped.
- **Use multifactor authentication** to guard against unauthorized access. This is especially important when accessing cloud-based resources or for any devices used for remote access.
- **Keep an eye out for phishing emails** that may appear to come from credible sources but are actually schemes to pull valuable information out of you and your employees.
- **Enable full disk encryption** on your laptops and other devices to protect them in the event they are stolen.
- **Have an action plan** in place before a cyberattack occurs so you do not lose time scrambling for resources and vendors who can help you shut it down and recover. Identify an experienced IT person who could help you in the event one occurs. Consult with attorneys who have experience in cyberlaw to understand your responsibilities when storing customer information.

Citations and links can be found in the citation summary ❯

PART II: YOUR STORE

TAKE A GROUND-LEVEL VIEW OF RETAIL SPACE RISKS

Your retail space is much more than just the four walls. You've invested your time and your money; it's your livelihood and your future. Make certain your store is as protected as it can be. Are you sure you have taken the right precautions to prevent against conditions where customers could slip and fall, possibly resulting in costly legal actions? Do you know where your water shut-off is located? Does your lease require you to have insurance coverage that might not be obvious for things you think are covered by your landlord? Staying ahead of these important issues can help keep your retail space thriving and safe.

When it comes to small retail stores, water damage, followed by customer slips, trips and falls and burglaries were the biggest loss drivers in 2016, according to CNA claim data. A small puddle on a tile floor, a gap in flooring or ripped carpeting all could prompt unsuspecting customers or employees to fall and injure themselves. About 10.642 million people visited their doctor's office after a fall in 2014, while 10.612 million visited the emergency room due to a fall that same year, according to the Centers for Disease Control and Prevention.[15]

IMPACT OF FALLS IN 2014

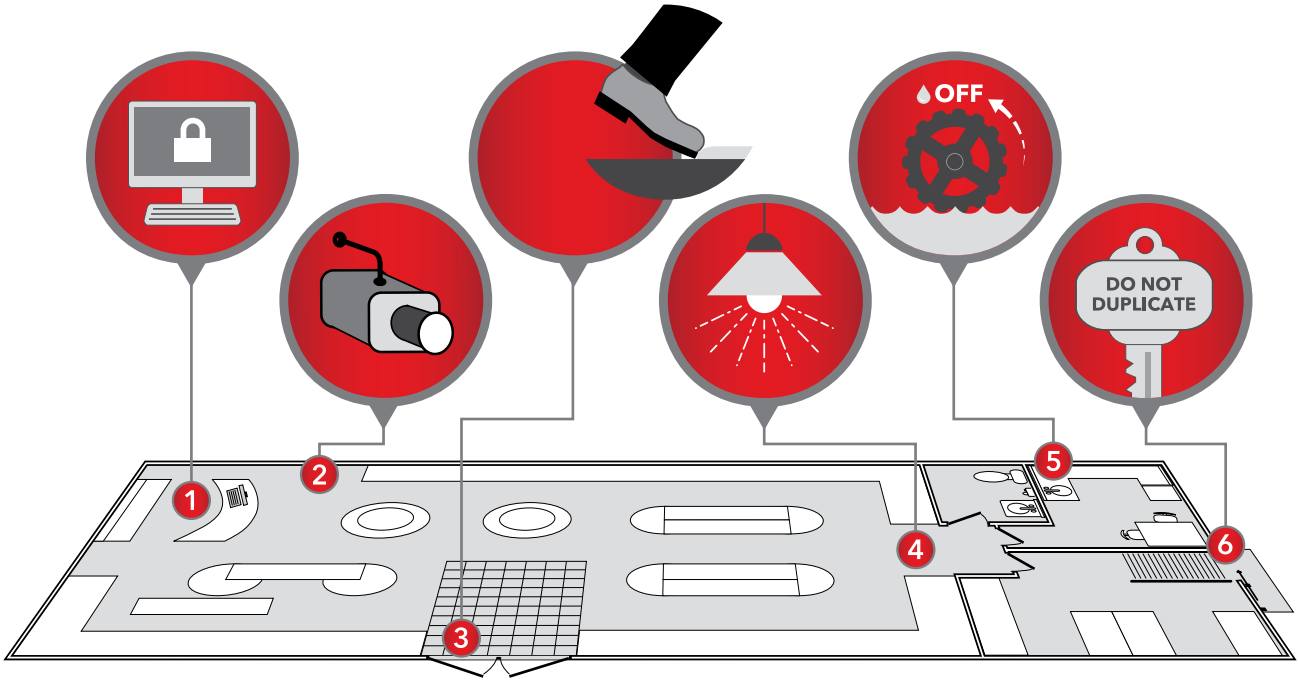
10,642,000
VISITS TO DOCTOR'S OFFICE

10,612,000
VISITS TO EMERGENCY ROOM

Citations and links can be found in the citation summary ❯

Scan Your Space: 6 Strategies to Safeguard Your Store

A customer slipping, a burst pipe, sewer backup, electrical surge, robbery or employee issue all can disrupt your customers' shopping experience. Ward off these interruptions by scanning your space for any potential hazards or threats, and by making certain you have the proper insurance coverage to help you bounce back from any unforeseen circumstances.



1 **Shield Your Data.** When was the last time you backed up your data? Do you have surge protection? Retailers must protect their computer systems from in-store catastrophes like a power surge, as well as from the schemes of hackers who could access your system remotely and steal your customer data.

2 **Discourage Robbers.** Be sure you are not setting up inviting spaces for would-be robbers. Install surveillance cameras. Post signs detailing your store policy that only small amounts of cash are kept in the register. Use a drop safe that allows employees to place large bills and excess cash inside, but not retrieve it. Removing the possibility of a large payout from a robbery may serve as a deterrent.

3 **Prevent Slips, Trips or Falls.** Slips, trips and falls are another top cause of loss for small retailers, so take steps to remove potential hazards. Address any change in elevation you find on the floor. Install slip-resistant strips on stairs and try to draw attention to them. Repair any cracks, holes or tears in flooring, and replace worn carpeting.

4 **Light It Up.** Insufficient lighting can be an accident waiting to happen, as a rip in the carpet or merchandise on the floor could be more difficult to see, and cause a customer or employee to trip. Dark corners also can provide hiding spots for criminal behavior.

5 **ID Your Water Shut-off.** Water damage is one of the top drivers for loss among small retailers. Know where your water valve shut-offs are — oftentimes, they may not even be in your retail space, instead locked behind a door that only maintenance personnel know how to access. That's not a good situation should a pipe burst or other water emergency occur. Train your employees how to respond and where to find the shut-off.

6 **Control Your Keys.** To protect your stock and space from unauthorized access and thieves, be strict in managing who has access to keys. Too many keys floating around raises the risk of one falling into the wrong hands.

A Most Vital Valve: Locate Your Water Shut-off

Plumbing emergencies can be expensive catastrophes. In some cases, the source of the water may not even be inside your space. "For tenants, it's very difficult for them to protect against water damage, which is the biggest cause of business interruption for the small business space because they don't have any control over their building, so they don't have any control over maintenance of the building," says CNA Risk Control Consultant Marjorie Gates. "They don't have any control over their neighbors."

One pre-emptive step to take:
Know ahead of time where the water shut-off is located, even if it's not in your space.

In many commercial buildings, the location of water control valves is top-secret information known only by maintenance personnel. But it can be problematic if the valves are behind the locked doors of mechanical closets or rooms, especially when most water damage leaks occur off hours. Improve your ability to respond by identifying valve locations ahead of time. Make sure the areas are marked in a highly visible way and properly maintained. Staff should be informed of the location and trained how to turn the water off.

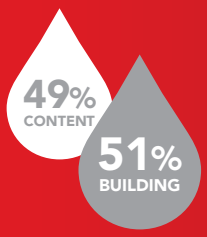
IT'S ALSO A GOOD IDEA TO:

- Label doors providing access to water control valves.
- Provide keys to these areas to designated staff working off hours.
- Determine when fire protection control valves can be safely shut off. This may require working with your local fire department on a plan to ensure fire is not present before shutting down the water supply valve.

THE PRICE TAG: What's the Potential Cost of a Water Emergency?

Water Damage by the Numbers

$37,812
Average loss due to water damage, according to CNA claim data from 2012-2016.



$18,464
average loss for water damage to the contents

$19,348
average loss for water damage to the building

The Dreaded Deluge: What to Do in a Water Emergency

With water leaking or flowing into your space, response time is crucial. You need to have a plan in place, one that you or your employees can activate immediately so valuable time isn't wasted.

- Ensure employees know how to report and respond to a water leak, blocked drain or overflow.
- If you have an identified exposure to sewer backup, the addition of a check valve in the affected line should be considered in order to prevent this type of exposure.
- Consider creating leak response kits with mops, towels, wet/dry vacuums, squeegees and wet floor warning signs.
- Identify a water damage restoration firm and establish an agreement with them. Make sure your plan includes authorization for staff to engage the outside resource when needed. This means immediate, emergency response 24/7.

Citations and links can be found in the citation summary ❯

Retail at the Ready: How Prepped Is Your Store for an Emergency?

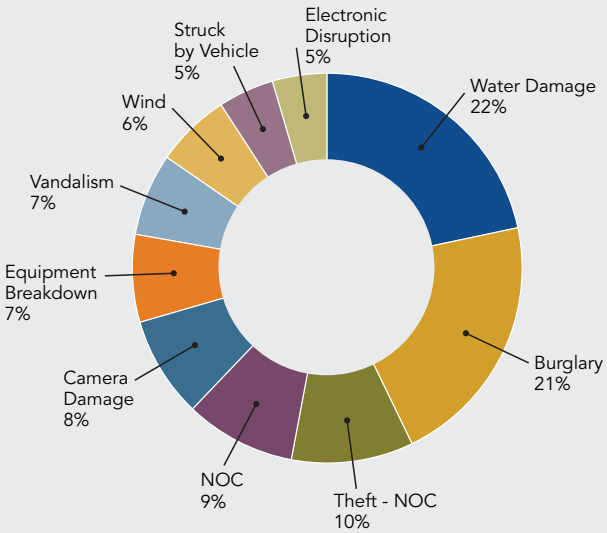
If your store is hit by a natural disaster or other emergency, you will be able to act more quickly if you've already done the thinking and preparation to develop a disaster response plan. In the moment, you won't have time to research cleanup companies, especially if your computer systems or stores are compromised.

Plus, the stress of the experience may make it easier for you to overlook important steps. That's why preplanning can be crucial to reduce the vulnerability of your retail store after a disruption. Make an emergency plan now, train your employees in what to do and keep hard copies of the plan on- and off-site.

Top Causes of Property Loss for Small Retailers

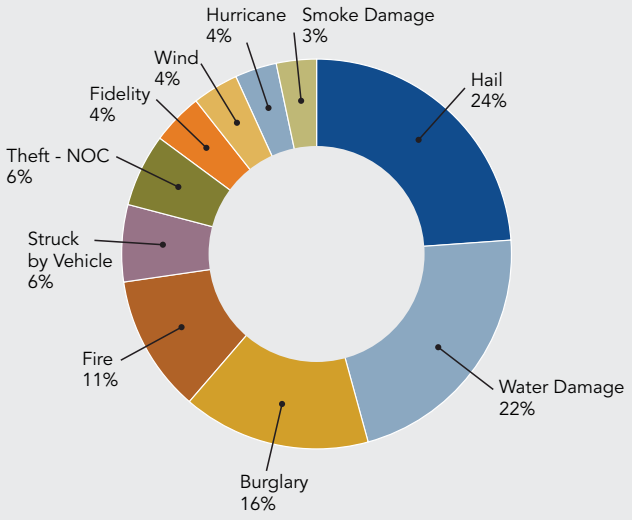
Frequency

The frequency chart speaks to how often claims are filed for each of these disruptions, according to 2016 CNA property claim data.



Severity

The severity chart shows which disruptions or events led to the most expensive property losses, according to 2016 CNA property claim data.



*Note: NOC=Not Otherwise Classified, or did not clearly fit into other categories.

What Should Be Included in an Emergency Plan?

Take a look at these tips:

- Identify types of losses that could affect your company and assess the degree of risk. What type of disasters could hit your area, your suppliers or customers?
- Identify operations crucial to survival and recovery.
- Make sure business records (sales data, customer lists, tax information, legal documents, etc.) are stored or are backed up at an off-site location.
- Ensure there are multiple vendors that can provide outsourced services in case of an emergency.
- Create a contact list of key vendors and business partners, and keep the list at an off-site location accessible by multiple employees rather than one person.
- Determine a meeting place in the event of an emergency.
- Ensure exits are clear and meet regulations to allow for proper evacuation. Determine where the staff could shelter in place during a weather emergency.
- Take into account security to protect people and property in case of an emergency.
- If applicable, ensure vendors have plans for payroll continuity.
- Work with vendors to ensure that employee data, such as personal and tax information, is stored at a secure, off-site location.
- Make sure those assigned tasks under the plan know what they are supposed to do.
- Train alternates in case backup help is needed.
- Practice crisis communication with employees.
- Invest in an alternate form of communication in case phones, email or computer networks go down or are inaccessible.
- Review the emergency plan at least annually and update as needed.

Source: CNA and FEMA.

INSURANCE CONSIDERATIONS

BUSINESS OWNERS POLICY (BOP). A Business Owners Policy, also known as a BOP, blends comprehensive property and general liability coverage for your small business into one policy. BOPs may include insurance for your building itself and your building personal property, such as your equipment, stock and furniture. Claims for slips, trips and falls and accidental water damage incidents would both be handled under a typical BOP covering property and general liability.

KNOW YOUR LEASE. When it comes to your retail lease, make sure you understand the fine print when it comes to your "buildout," or any improvements made to the inside of your retail store to prepare it for operations. Do you own the fixtures and components of the buildout or does the building owner? And if you own it, does the lease transfer the ownership of fixtures and other components to the landlord at some point? Who is responsible for insuring the fixtures and finishes in the buildout? Retailers should take care to understand all the details of their lease when it comes to their insurance responsibilities.

TAKEAWAYS

- **Scan your space** for possible slip, trip and fall hazards.
- **Keep up** with housekeeping and maintenance.
- **Know where your water shut-off is**, and train employees how to react to a water emergency.
- **Develop an emergency plan**.

PART III: YOUR EMPLOYEES

YOU'RE THE BOSS: 2018 HANDBOOK FOR SMALL RETAIL EMPLOYERS

From interviewing and training, to building teams and enforcing policies, being an employer brings with it a host of issues. Trustworthy, dependable employees are crucial to your store success, but it's also important to guard against any problems that can be posed by those who may ultimately no be trustworthy and dependable.

Retailers "tend to be more trustful of their employees," says CNA Risk Control Consultant Marjorie Gates. Employee theft ranked as the top cause of retail shrink in the U.S., accounting for 45 percent of the total loss, according to the 2016 Global Retail Theft Barometer.[16] Retailers blamed weak pre-employment screenings, reduced supervision of sales associates, a reliance on more part-time workers and the ease with which one can resell stolen items, according to the report.

One small business learned the hard way how vulnerable it was to employee theft when the office manager went on vacation. Another employee who was filling in noticed something strange about the company credit card statements. It turned out the vacationing employee had stolen hundreds of thousands of dollars using the company credit card. Luckily, the small business owners had employee dishonesty coverage through their insurance policy, which covered some, but not all of the loss. As for the office manager? She did some prison time for the creative yet highly unauthorized use of company credit.

Citations and links can be found in the citation summary ❯

Background screenings can be a good idea, particularly if you are stocking higher valued items, such as electronics or cellphones. Inside knowledge sometimes makes it easier for employees to strike because they know the schedule, the patterns and how to dismantle alarm systems or avoid triggering other security mechanisms. Cameras also are recommended in higher value spaces.

To prevent insider theft, proper controls around inventory and cash flow management are important. Solid accounting practices can alert owners to possible financial fraud or wrongdoing. Retailers are encouraged to implement best practices with their cash flow, such as requiring two people to sign checks above a certain dollar value and making sure employees handling financials or cash are supervised.

Basics for the Boss: **The Job Application**

- The application form should be developed with the assistance of legal counsel.
- The form should declare that all false statements are grounds for rejection or immediate termination.
- A release and authorization form, signed by the applicant, will allow for verification of all information on the application form. This form also should provide authorization for obtaining criminal background and credit history checks.
- The application form should be signed by the applicant.
- The application should include, but not be limited to, the following: biographical information (such as name, address, driver's license and Social Security numbers); previous addresses and whether the applicant has worked under other names and/or Social Security numbers; education; employment history; and references.

6 Ways to Prevent Employee Theft

1. Establish a written policy that outlines employee responsibilities, standards of honesty, general security procedures and consequences if not followed. Ensure new employees read the policy, understand it and sign it as a condition of employment.
2. Follow strict hiring practices. Verify all information and contact all references listed on an application.
3. Keep and maintain accurate records on cash flow, inventory, equipment and supplies. Have it reviewed regularly by someone other than the person responsible for maintaining it.
4. Limit access to keys, the safe, computerized records and alarm codes. Engrave "DO NOT DUPLICATE" on store keys. Change locks and access codes when an employee is terminated.
5. If internal theft is discovered, take action quickly. Contact your local law enforcement agency and be sure to send a message to your employees that theft will not be tolerated.
6. Reward employees for uncovering security problems.

Set the Ground Rules

An employee handbook is essential, and retailers should have employees sign the handbook as confirmation that the person was made aware of the policies inside. That makes it easier for employers if they do need to take disciplinary action or move toward termination. "You can't be there all the time to understand what they're doing, so make sure you have an employee handbook, make sure you set the ground rules of what is or is not a perk of the job. Helping yourself to free coffee is fine. Helping yourself to free shoes is not fine," says Greg Dasher, Vice President for Small Business Underwriting for CNA.

As the boss, it's your responsibility to provide your employees with safe work conditions and proper training. Even small retail spaces tend to have a storage space or room, so retailers should be sure to train employees on practices such as proper lifting and ladder safety. Slips, trips and falls are a concern for employees as well as your customer. The retail trade is particularly affected by workplace injuries, with 123,770 incidents that led employees to need days away from work in 2015, according to the U.S. Bureau of Labor Statistics.[17]

THE PRICE TAG: What's the Potential Cost for Employee Problems and Misbehaviors

Employment Practices Liability Issues by the Numbers

$15,131

Average loss due to an Employment Practices Liability issue, according to CNA claim data for 2012-2016. Employment Practices Liability problems can encompass a range of negative workplace behaviors, such as harassment, retaliation or discrimination.

+

The Essentials of **Your Employee Handbook**

The retail employee handbook can cover a range of policies and issues, including, but not limited to:

- Hiring and firing.
- Employee behavior expectations (promptness) as well as rules about the workplace being a drug- and alcohol-free environment.
- Maternity policy.
- Disability policy.
- Vehicle use — especially if employees are making drop-offs. You also can detail the mileage reimbursement policy and procedures following an accident.
- Prohibition of harassment/discrimination.
- Use of corporate credit cards (if any employees have access to them).
- Cash management and financial policies to cover who has access to cash, how it's handled and if a manager or supervisor has to sign off at the end of a shift.
- Computer access and social media guidelines.
- Key access — who can get into the building and when. No copying keys.
- Inventory management policies to lay out who manages it and how it works.

Citations and links can be found in the citation summary ❯

INSURANCE CONSIDERATIONS

EMPLOYMENT PRACTICES LIABILITY. If you have more than one location, you cannot be at each location around the clock, which means you can't police behavior all the time by yourself. That manager who seems really great when you're in the store could be exhibiting less-than-exemplary behavior in your absence. Employment practices liability insurance covers many losses arising out of employee disputes where harassment, discrimination or retaliation may be involved. Employee handbooks don't eliminate your exposure to employment practices liability problems. Business liability policies generally have a standard exclusion for employment practices liability exposures, or may only offer limited coverage. You should verify any policy you consider is adequate to meet the needs of your retail operation.

WORKERS' COMPENSATION. Workers' compensation insurance offers coverage for medical expenses and wage replacement for employees injured on the job. Even in a small store setting, employees can be injured from slips, trips or falls, resulting in time when they are unable to work. Going without workers' compensation coverage could result in penalties and charges. Laws requiring workers' compensation insurance vary by state.

Some insurance companies offer different workers' compensation pay arrangements that are worth investigating. Typically companies require businesses to pay a larger portion of the workers' compensation premium up front. If the business owner hires additional sales associates over the course of the year, the insurance premium may increase to cover that, meaning the owner will owe even more come renewal time. Some insurance companies offer workers' compensation in a pay-as-you-go arrangement, eliminating the requirement for a down payment and allowing employers to pay as they pay their employees. This can be essential for retail, which is more cyclical in nature, tending to boost staffing during busy seasons such as the holidays, and reducing it during lighter times. Under these scenarios, if a retailer paid accurately throughout the year, the guesswork and surprise premium increases should be eliminated.

TAKEAWAYS

- **Spell out your expectations** and policies in a handbook and have employees sign it.
- **Include solid checks and balances** when it comes to the handling of cash and inventory.
- **Protect your employees** through safety training.
- **Be sure you have the right insurance** coverage for yourself and your employees.

PART IV: YOUR ASSETS

ASK THE RIGHT QUESTIONS

Think about your business in two parts — there's the property itself, with the four walls and roof of the building, and then there's everything inside that would be considered your "business personal property." Business personal property includes your furniture, computer equipment, inventory, paper records and the like. When it comes to the assets of your small retail space, you need to think proactively to be sure you will have the resources to restock and reboot as soon as possible in the event of a loss.

If you suffer damage from a weather disaster, or an employee makes off with a decent amount of inventory, how would you respond? Do you have contacts for suppliers that could quickly replenish your stock? Identify these vendors ahead of time. Doing so will save vital time and energy during a stressful period and help you open again as quickly as possible.

THE PRICE TAG: What's the Potential Cost If My Business Personal Property Is Damaged or Stolen?

Asset Losses by the Numbers

$15,476

Average loss for a Business Personal Property claim, according to CNA claim data for 2012-2016. Business Personal Property includes items like your tables, desks, chairs and inventory.

Again, solid data management and backup can strengthen your resiliency to a disaster. Those retail business with organized inventory systems that are backed up tend to rebound quicker. "If Retail Space A experiences a business loss and has their inventory records really well managed and has their accounting records really well managed, and has it all backed up, they're going to be in a better position to get a foothold and get back up and running faster as opposed to Retailer B that doesn't have that," Gates says.

Don't Be Predictable

To protect assets such as cash and securities, retailers should be careful not to set a specific schedule for tasks like money drops to the bank. Most small retailers won't have an armed security truck pulling up to collect their deposits; instead an employee will be dropping off the money. Scatter the schedule so you don't create vulnerability by having someone deposit money at 9:30 a.m. every Tuesday, allowing potential thieves to track your pattern. Conduct background checks on anyone who is dealing with money.

The Key to **Store Safety**

To protect your stock, it's important to manage who has access to keys. You don't want too many keys floating around, increasing your risk of unauthorized access and theft. Follow these steps to tighten access to your retail space:

- Avoid key duplication.
- Keep records on every key handed out, and to whom.
- Whenever a key is lost or an employee leaves the firm without turning in his or her key, re-key the locks.
- Have one key and lock for exterior doors and a different key and lock for the office.
- Have a code for each key so that it does not have to be visibly tagged and allow only those authorized to know the specific lock that key fits.
- Take a periodic inventory of keys.

Your Robbery Risk: 12 Steps to Reduce Your Exposure

1. Greet every person who enters the business in a friendly manner to discourage a would-be criminal.
2. Keep windows clear of displays or signs and make sure your business has good lighting. Eliminate any blind spots in your store that may hide a robbery in progress.
3. Provide information about your security systems to employees only on a need-to-know basis. Instruct your employees to report any suspicious activity or person immediately and write down the information for future reference.
4. Keep small amounts of cash in the register to reduce losses. Use a drop safe that allows employees to drop large bills and excess cash but not retrieve it. Post signs alerting would-be robbers of this procedure. Place excess money in a safe or deposit it as soon as possible.
5. Make bank deposits often and during business hours. Don't establish a pattern; take different routes at different times during the day. Ask a police officer to escort you to the bank whenever possible.
6. Ask local law enforcement what to do if you are robbed. Make sure your address is visible so emergency vehicles can easily find your business.
7. Do not release personal information to strangers.
8. Keep purses and personal valuables locked in desks or lockers.
9. Install a robbery alarm.
10. Place a surveillance camera behind the cash register facing the front counter. Replace videotapes regularly.
11. Don't use marked "money bags" that make it obvious to would-be robbers you are carrying money for deposit.
12. Install adequate indoor and outdoor lighting.

+

Shoplifters Beware: **Protect Your Inventory**

Shoplifting remains a concern, as it was responsible for 36 percent of retail shrink in the U.S., according to the 2016 Global Retail Theft Barometer.[18]

- Train employees how to reduce opportunities for shoplifting and how to apprehend shoplifters. Work with law enforcement to teach employees what actions may signal shoplifting.
- Keep the store neat and orderly. Mirrors can be used to eliminate "blind spots" in corners. Merchandise should be kept away from store exits to prevent grab-and-run situations.
- Keep displays full and orderly so employees can see at a glance if something is missing. Keep expensive merchandise in locked cases. Limit the number of items employees remove at any one time for customers to examine.
- Design the exits of the business so all persons must pass by security personnel or store employees. You may want to use an electronic article surveillance system or other inventory control devices.
- The cash register should be inaccessible to customers, locked and monitored at all times. Place it near the front of the store so employees also can monitor customers coming and going.
- Dressing rooms and restrooms should be watched at all times. Keep dressing rooms locked and limit the number of items a customer can bring into the room.

Citations and links can be found in the citation summary ›

Burglary Prevention Tips

Burglary was to blame for 21 percent of CNA property claims filed by small retailers in 2016, according to CNA data. Make sure your space is equipped with:

- Suitable locks
- Pin tumbler locks with at least seven pins
- Double cylinder deadbolt locks
- An appropriate alarm system
- Suitable exterior and interior lighting. Exterior lighting is particularly important when materials, equipment or vehicles are outside.
- Windows that are easily reached from the ground or adjacent structures that do not front main roads should be blocked or protected. Heavy metal window screens or grating are an inexpensive way to protect show windows.
- All exterior doors should have a metal facing or solid metal construction. The door frame should also be of substantial construction and be securely mounted to the structure.
- When used in exterior doors, windows, display windows and interior showcases, burglar-resistant glass can deter burglars.

INSURANCE CONSIDERATIONS

ASK THE RIGHT QUESTIONS TO KNOW WHAT'S COVERED. When evaluating your insurance options, think through your daily operations. What if an employee who is dropping off the day's deposit to the bank stops at the store for a beverage and the bag is stolen from his or her car? Are you covered for that? Understand whether your policy would cover money and securities on the way to the bank or if that is excluded. A business insurance policy may cover $10,000 in money and securities if the theft occurs in the store, but only $5,000 on the way to the bank, as not all policies include off-premises coverages.

Consider whether your stock is covered in transit. Are you, as the retailer, responsible as soon as it leaves the distributor warehouse, or does responsibility shift to you once it arrives at your location? Read your contracts closely to be clear when you are responsible for your stock. Are you covering it once it's shipped to the customer, from your doorstep to theirs? Does it matter who or what type of vehicle is transporting it?

ACCURATELY VALUE YOUR ASSETS. Be sure to have enough coverage for your assets. You don't want to experience a roof leak or a sewer backup in your store, find your stock ruined and then learn you didn't buy enough coverage to replace the furniture and inventory you actually had in the store. Properly valuing the amount of your business personal property is important to avoid situations that make recovery of your retail store more difficult.

Be aware of business insurance policies that have co-insurance penalties for underinsuring your property. If $80,000 in building coverage is purchased, but the value of the property is $100,000, the building is underinsured. You don't want to be surprised when filing a fire claim to find that you may not be paid that $80,000 because you didn't buy adequate coverage for the property value. Some insurers waive that penalty, so be sure to ask.

TAKEAWAYS

- **Keep up-to-date records** on who has keys to the store.
- **Properly value your inventory** and contents of your store for insurance coverage purposes.
- **Protect your employees** through safety training.
- **Be sure you have the right insurance** coverage for yourself and your employees.

CONCLUSION

RESILIENT RETAILERS STRENGTHEN THEIR STORES FOR 2018

Any interruption to your retail store operations can hurt your bottom line. Consider what happens if a pipe bursts on a cold night, and you arrive to find water has been leaking throughout your business most of the night. Your inventory and the wood flooring is damaged. Water remediation and cleanup work has been known to take up to three months for CNA retail claimants with this level of damage. Some have experienced inventory and contents losses of more than $300,000. A business interruption loss — or a claim filed to keep a business going while the flooring is repaired and the store is reopened — may total more than $200,000. That's not an easy amount to absorb without adequate coverage.

Keep in mind that for every dollar you lose in damaged equipment, there also are intangible costs to consider, such as lost profits and damage to retail customer relationships while your doors are shuttered.

Be sure to work with an experienced insurance company that will tailor a business owners policy to the needs of your specific business. If more of your retail operation is moving online, consider whether you need to increase cyber coverage. Evaluate whether you are properly covered for employee issues. Your store needs can be unique, but your business owners policy should be customizable to allow you to sleep better at night, knowing one unpredictable event does not have to mean the end of the retail store you've worked so hard to build.

With proactive planning, you can feel more secure that your customer data, your store, your employees and your assets are in the best possible position to weather the future so you can concentrate on strengthening your retail business for an evolving retail environment.

Visit Retail on www.cna.com for more resources.

Citation Summary & Resource Links

1 United Parcel Service, "UPS Pulse of the Online Shopper," June 2017, https://pressroom.ups.com/assets/pdf/pressroom/white%20paper/UPS_2017_POTOS_media%20executive%20summary_FINAL.pdf, accessed Sept. 12, 2017.

2 Robin Sidel, "Home Depot's 56 million card breach bigger than Target's," The Wall Street Journal, Sept. 18, 2014, https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

3 U.S. Department of Justice, "Russian cyber-criminal convicted of 38 counts related to hacking businesses and stealing more than two million credit card numbers," Aug. 25, 2016, https://www.justice.gov/opa/pr/russian-cyber-criminal-convicted-38-counts-related-hacking-businesses-and-stealing-more-two; Nicole Perlroth,"Russian Hacker Sentenced to 27 Years in Credit Card Case," The New York Times, April 21, 2017, https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html?mcubz=3.

4 Identity Theft Resource Center, "Data Breach Reports: 2016 End of Year Report," http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf, accessed Aug. 29, 2017.

5 National Small Business Association, "2015 Year-End Economic Report," http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf, accessed Aug. 29, 2017.

6 National Small Business Association report.

7 Identity Finder, "Sales Drop as Corporate Data Breaches Rise According to New Study from Identity Finder," April 29, 2014, http://www.prnewswire.com/news-releases/sales-drop-as-corporate-data-breaches-rise-according-to-new-study-from-identity-finder-257140751.html.

8 Martyn Williams, "Data breach that hit Jimmy John's is larger than first thought," Computerworld, Sept. 26, 2014, https://www.computerworld.com/article/2687802/data-breach-that-hit-jimmy-johns-is-larger-than-first-thought.html.

9 U.S. District Court, Central District of Illinois class action complaint, Nov. 6, 2014, http://pdfserver.amlaw.com/nlj/capl%20jimmyjohns%201110.pdf.

10 PCI, "Maintaining Payment Security," https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security, accessed Sept. 15, 2017.

11 Source: PCI Security Standards Council

12 CNA cyber claims data, 2012-2016.

13 Source: U.S. Department of Justice Cybersecurity Unit, "Best Practices for Victim Response and Reporting of Cyber Incidents," April 2015.

14 Wasp Barcode Technologies, "State of Small Business Report," https://www.waspbarcode.com/small-business-report, accessed Aug. 29, 2017.

15 P. Rui, E. Hing, T. Okeyode, Centers for Disease Control and Prevention, "National Ambulatory Medical Care Survey: 2014 State and National Summary Tables," https://www.cdc.gov/nchs/data/ahcd/namcs_summary/2014_namcs_web_tables.pdf; P. Rui, K. Kang, Centers for Disease Control and Prevention,
"National Hospital Ambulatory Medical Care Survey: 2014 Emergency Department Summary Tables,"
https://www.cdc.gov/nchs/data/nhamcs/web_tables/2014_ed_web_tables.pdf.

16 Checkpoint Systems, "Latest Global Retail Theft Barometer Study Finds U.S. Retail Shrink Up,"
Nov. 4, 2015 press release, http://us.checkpointsystems.com/news-events/news-item/latest-global-retail-theft-barometer-study-finds-u-s-retail-shrink-up-2/.

17 U.S. Department of Labor, Bureau of Labor Statistics, "Nonfatal Occupational Injuries and Illnesses Requiring Days away from Work, 2015,"
Nov. 10, 2016, https://www.bls.gov/news.release/pdf/osh2.pdf.

18 Checkpoint Systems.