The Security of Confidential Documents in the Workplace

Study conducted by Ponemon Institute
Results sponsored and reported by Shred-it
September 2019

Ponemon Institute©
Research Report

A PARTNERSHIP FOR DOCUMENT SECURITY

As the world becomes more digital, it is easy to think about information security in purely digital terms. Yet despite office modernization, paper is still a big part of the workflow. It is safe to assume that almost all documents exist in the physical world at some point in their lifecycle; whether it is to share with colleagues, review a draft, or to print a hard copy for file storage. Information security programs that focus solely on digital protection are really only doing **half** the job.

As an industry-leading expert in document security, Shred-it has partnered with Ponemon Institute to research and quantify the often-overlooked risks that paper documents present to an organization's overall information security. For nearly two decades Ponemon Institute has been conducting research on data protection and emerging information technologies and is considered the leading authority on the risks and liabilities that organizations face when it comes to protecting and securing confidential information.

This report underscores the real risks organizations face if they neglect to secure their printed documents and it provides helpful suggestions as to how they can protect their confidential information more effectively.

CONTENTS

EXECUTIVE SUMMARY

It does not take the stealth and sophistication of a cyber attacker to cause a data breach. A careless employee leaving a sensitive document in a communal printing tray or a malicious insider intent on stealing information in documents that have not been properly destroyed can result in the loss or theft of critical information assets.

Sponsored by Shred-it, the research reveals the inadequacies in organizations' policies regarding the protection of confidential documents in the workplace. Ponemon Institute surveyed 650 individuals who work in both IT security and non-IT positions in North American organizations. All respondents are knowledgeable about their organization's strategy for the protection of confidential and sensitive information.

Many data breaches involve the loss or theft of information contained in paper documents and electronic devices.

According to the findings, 68% of respondents say their organization experienced a data breach in the past 12 months. Of these respondents, 69% say one or more of these data breaches involved the loss or theft of paper documents or electronic devices containing sensitive or confidential information, as shown in Figure 1.

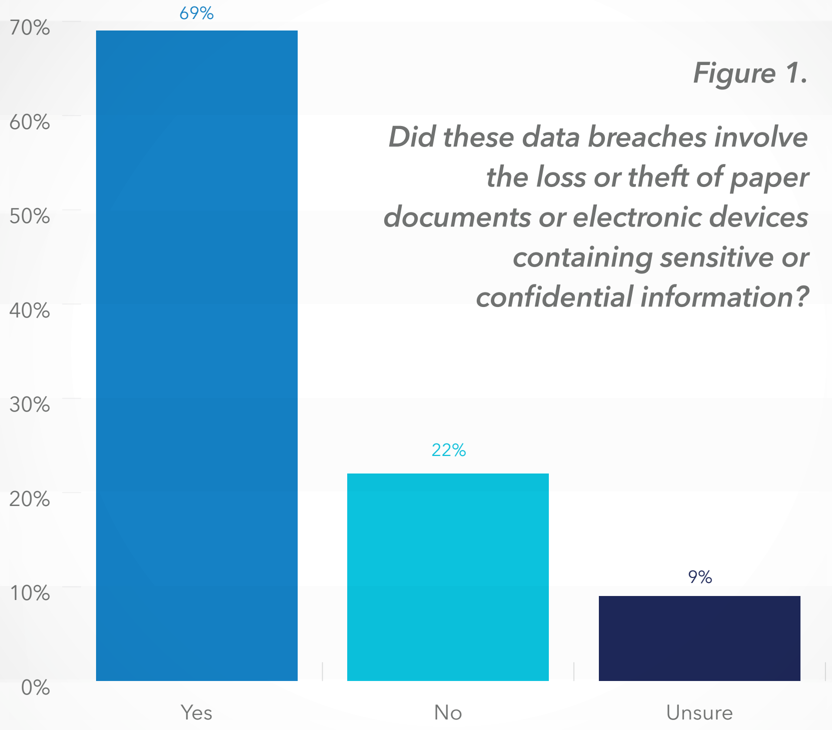


Figure 1.

Did these data breaches involve the loss or theft of paper documents or electronic devices containing sensitive or confidential information?

Why documents containing sensitive and confidential information are at risk.

There is a security disconnect in the protection of confidential documents.

The chief information security officer and chief security officer are most responsible for protecting confidential information, according to 21% and 18% of respondents. However, they rarely have responsibility for granting access to paper documents or electronic devices containing sensitive or confidential information.

Most companies are not training employees about secure disposal.

Only 45% of respondents say their organizations have a process for disposing of paper documents containing sensitive or confidential information after they are no longer needed. Less than half (46% of respondents) say their organizations are training employees about the steps they should be taking to ensure documents are appropriately disposed of. Furthermore, very few respondents say their organizations automate restrictions to print from specific devices and to print specific files, 29% and 27%, respectively.

Organizations are not taking basic precautions to prevent the loss or theft of confidential documents.

Confidential documents are not secure because few organizations are requiring employees and contractors to lock their desks and file cabinets (38% of respondents). Only 33% of respondents say they prevent unauthorized access to document storage facilities and 31% of respondents say a clean desk policy is enforced.

Why documents containing sensitive and confidential information are at risk.

The lack of policies and training for the secure disposal is having an effect on respondents' confidence in keeping confidential documents secure.

Only one-third of respondents have confidence in their organizations' ability to govern the use, protection and disposal of paper documents. Fewer respondents (26%) have confidence in having visibility into what employees are doing with confidential documents.

Organizations are unable to restrict employees' access to paper documents they should not see.

Most respondents (61%) are unsure or disagree that the protection of paper documents is just as important as the protection of electronic records. As a result, 60% of respondents strongly agree or agree that employees, temporary employees and contractors have access to paper documents that are not pertinent to their role or responsibility.

Only 37% of respondents strongly agree or agree that it is convenient for employees and contractors to destroy paper documents with sensitive and confidential information. The fact that only 41% of respondents agree employees and contractors recognize the types of information that are sensitive or confidential demonstrates the lack of training in organizations.

Why documents containing sensitive and confidential information are at risk.

Confidential documents are left in plain sight.

65% of respondents are concerned that employees or contractors have printed and left behind a document that could lead to a data breach. Even more respondents (71%) admit they have picked up or seen a paper document in a public space that contained sensitive or confidential information.

More than half (51% of respondents) say they either keep the document or throw it in the garbage.

Conversely, only 33% of respondents say they shred the document after reviewing it.

Sensitive or confidential information is exposed because of sending and receiving emails not intended for the recipient.

77% of respondents admit to sending emails containing sensitive or confidential information to the wrong person. 88% of respondents say they have received such emails.

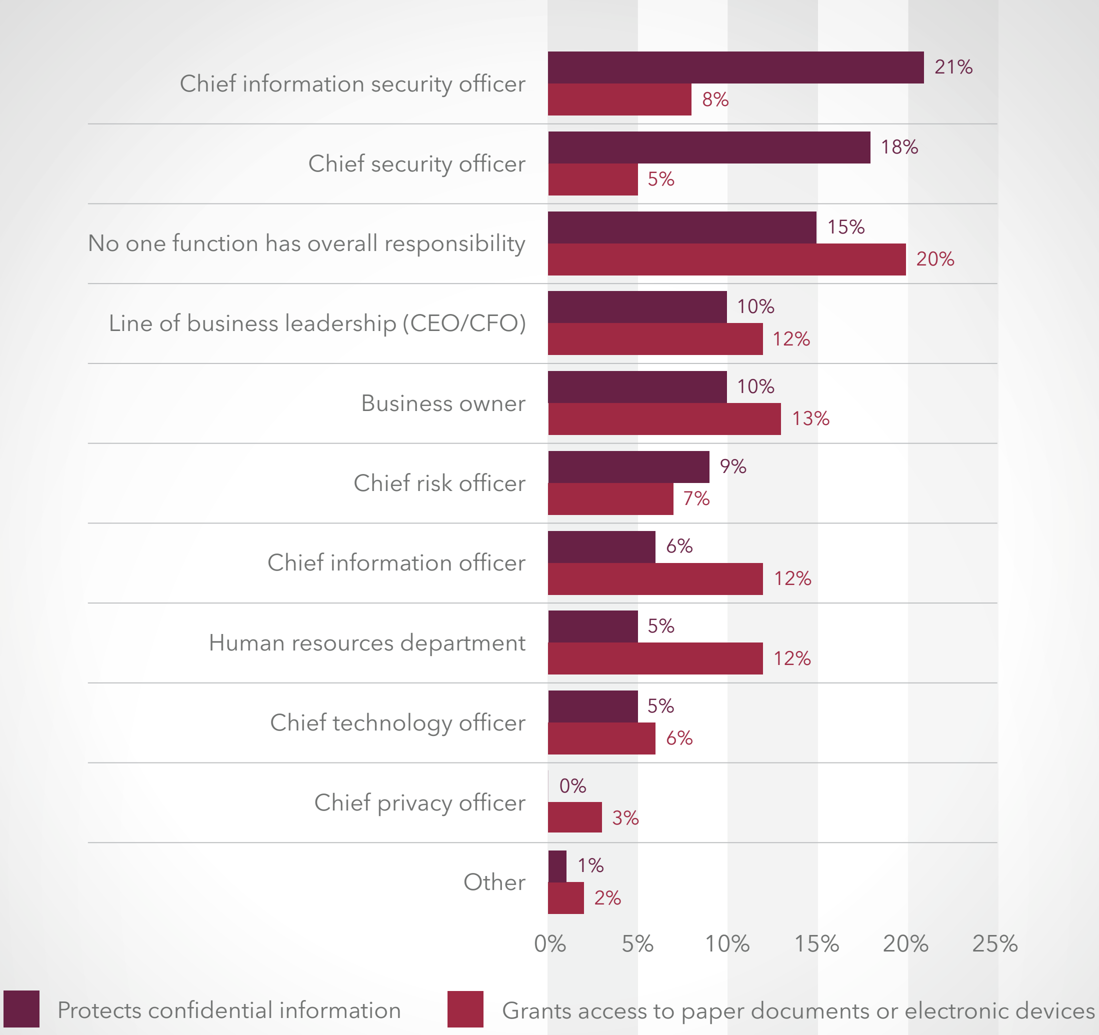
KEY FINDINGS

Steps taken to protect confidential information in paper documents and electronic devices.

There is a security disconnect in the protection of confidential documents.

According to Figure 2, the chief information security officer and chief security officer are most responsible for protecting confidential information, according to 21% and 18% of respondents. However, they rarely have responsibility for granting access to paper documents or electronic devices containing sensitive or confidential information. Additionally, 15% of respondents say that no one function has overall responsibility.

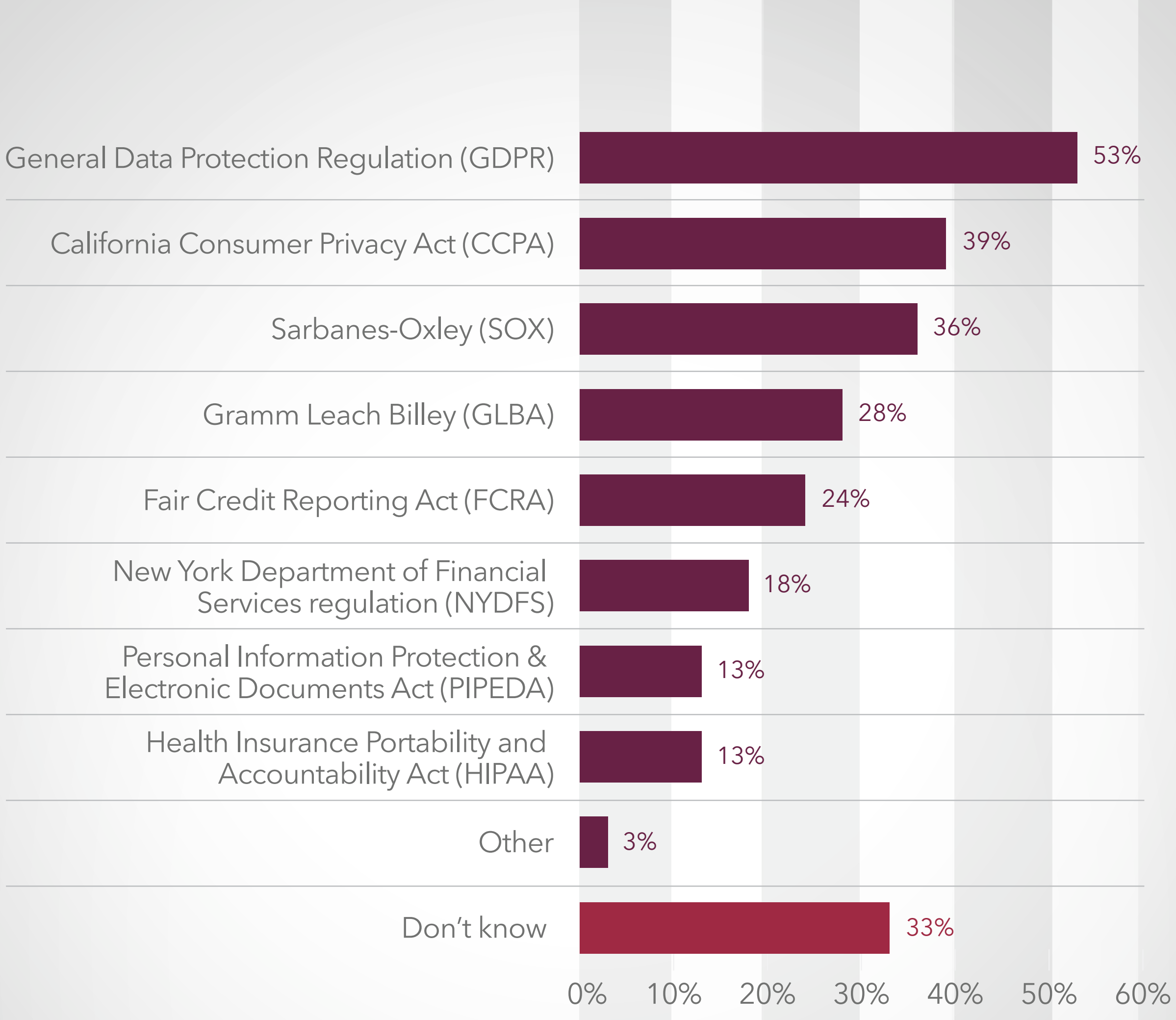
Figure 2. Who protects and grants access to paper documents and electronic devices?



Many respondents are not aware of the privacy laws and regulations their organization must comply with.

As shown in Figure 3, 53% of respondents say their organizations must comply with the GDPR. However, one-third of respondents say they do not know the regulations affecting their handling and protection of personal information. Of the 67% of respondents who do know, only 37% of respondents are knowledgeable about the potential fines and penalties as a result of non-compliance with these regulations.

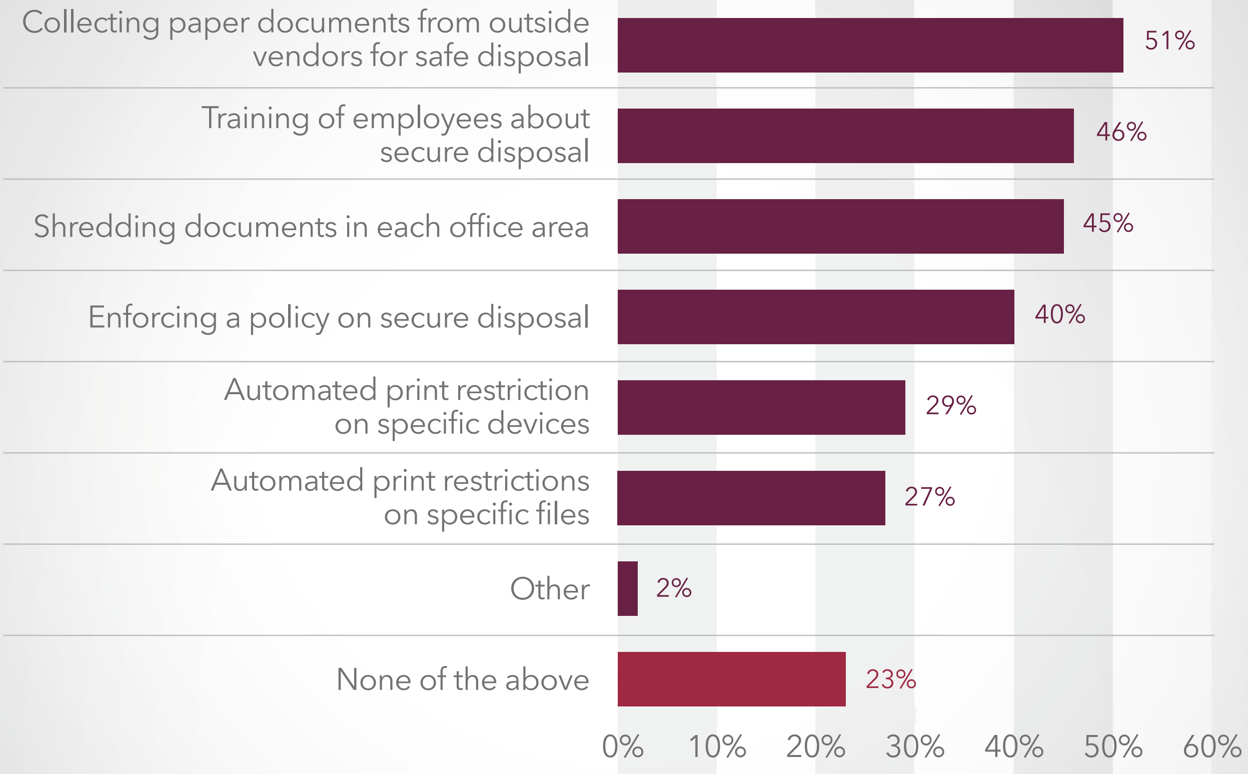
Figure 3. What privacy laws and regulations does your organization comply with?
More than one response permitted.



Most companies are not training employees about secure disposal.

Only 45% of respondents say their organizations have a process for disposing of paper documents containing sensitive or confidential information after they are no longer needed. Figure 4 presents the activities these respondents say their organizations have in place to safely dispose of paper documents. Less than half (46% of respondents) say their organizations are training employees about the steps they should be taking to ensure documents are appropriately disposed of. Furthermore, very few respondents say their organizations automate restrictions to print from specific devices and to print specific files, 29% and 27%, respectively.

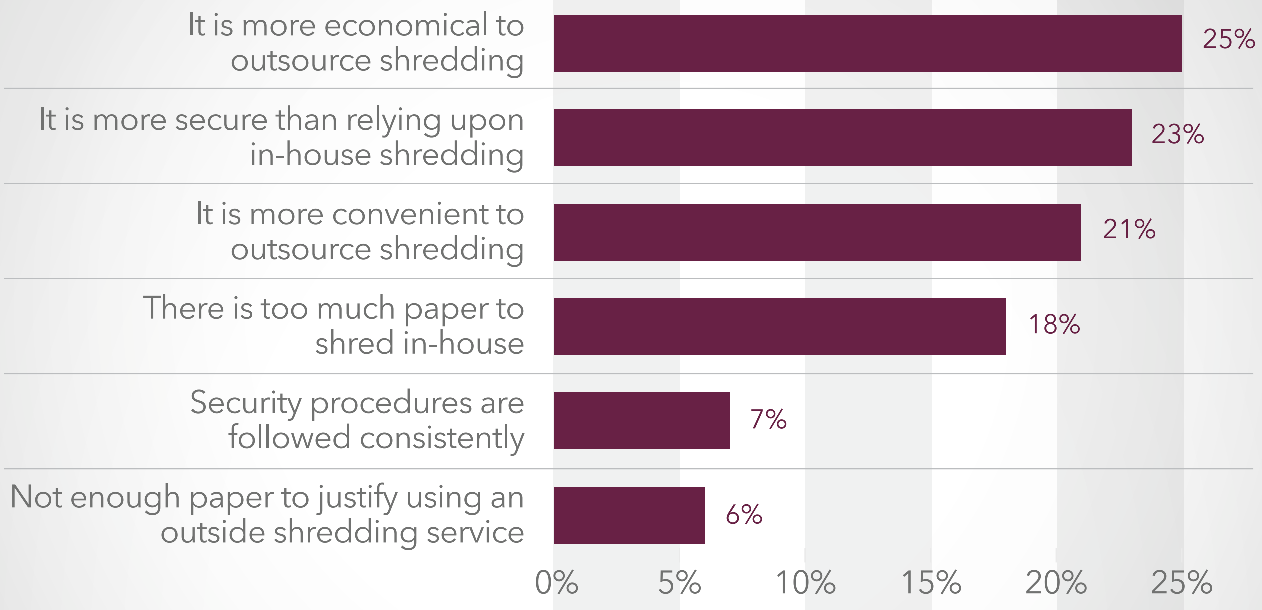
Figure 4. How does your organization safely dispose of paper documents?
More than one response permitted.



Saving money, better security and convenience are the top reasons for using an outside shredding service.

34% of respondents are using an outside shredding service. Reasons for outsourcing shredding are economics (25% of respondents), it is more secure than in-house shredding (23% of respondents) and more convenient (21% of respondents), as shown in Figure 5.

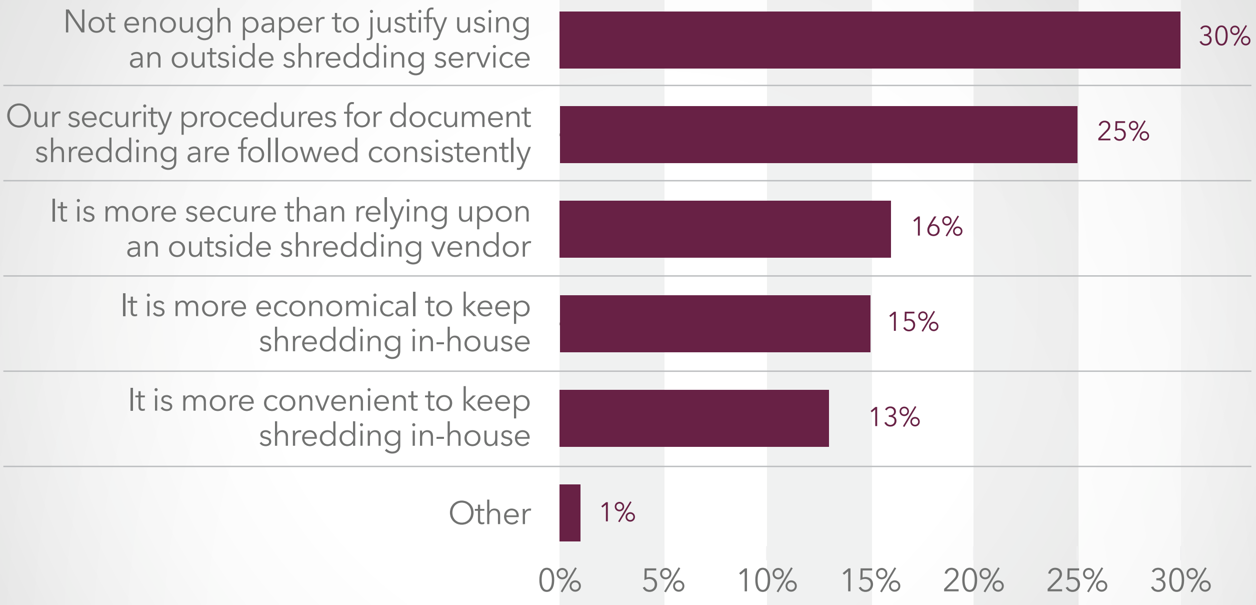
Figure 5. Why does your organization use an outside shredding service?



Not enough paper to shred is the primary reason for not using an outside shredding service.

66% of respondents say their organizations do not use such a service. According to Figure 6, 30% of respondents say there is not enough paper to shred. Another 25% of respondents say their security procedures for document shredding are followed consistently.

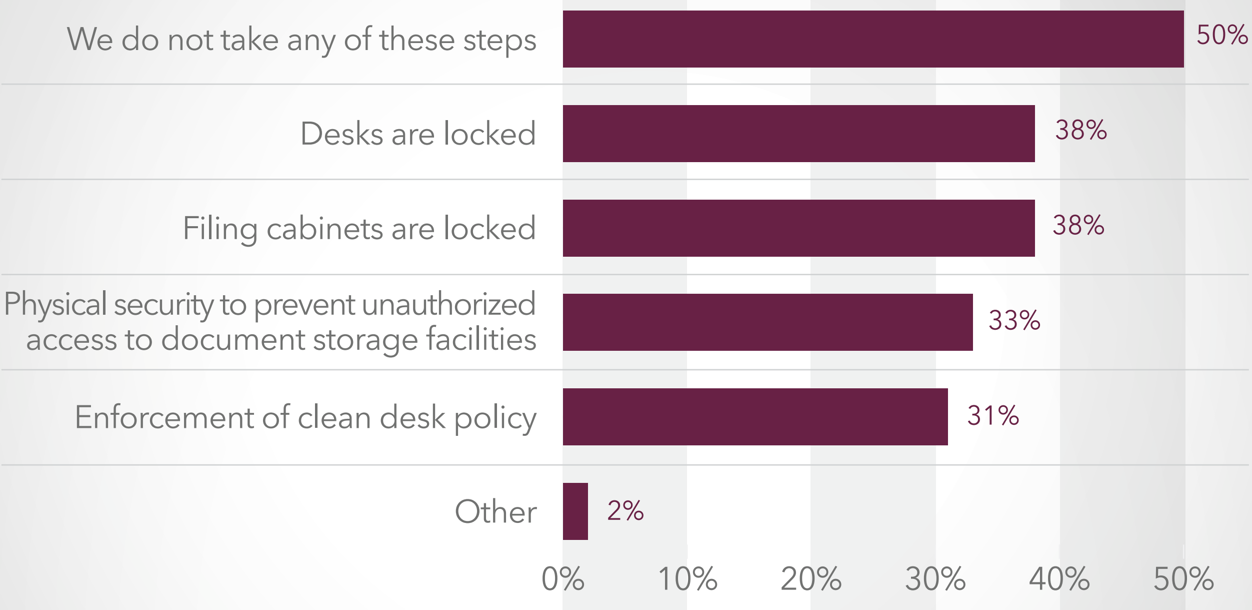
Figure 6. Why does your organization not use an outside shredding service?



Organizations are not taking basic precautions to prevent the loss or theft of confidential documents.

Confidential documents are not secure because few organizations are requiring employees and contractors to lock their desks and file cabinets (38% of respondents). Only 33% of respondents say they prevent unauthorized access to document storage facilities and 31% of respondents say a clean desk policy is enforced, as shown in Figure 7.

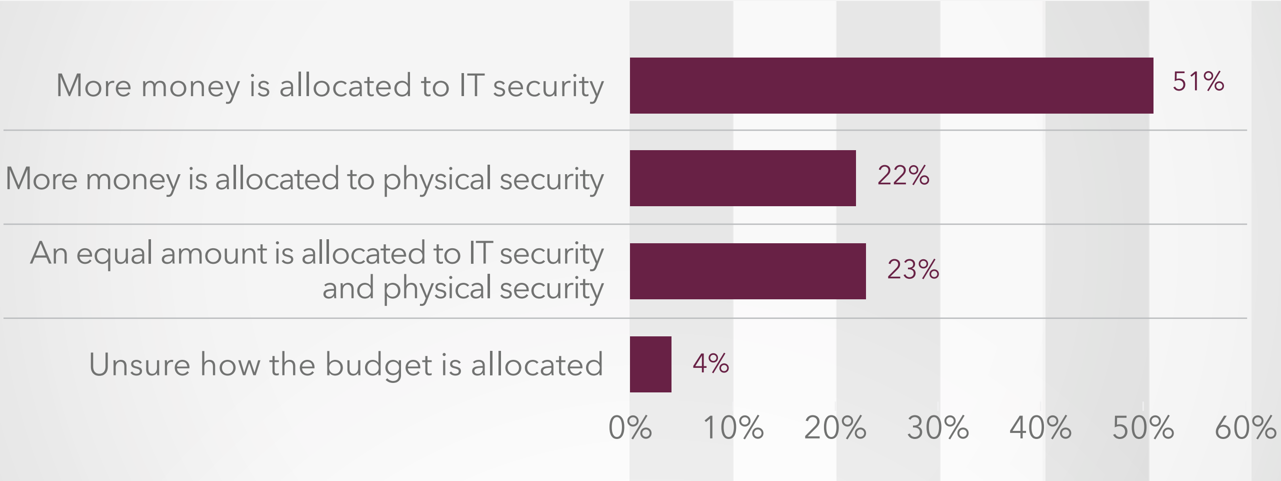
Figure 7. Which action best describes how your organization restricts employee or contractor access to physical paper documents? More than one response permitted.



More money is allocated to IT security than physical security.

The average annual budget for IT and physical information security is $2.6 million. As shown in Figure 8, 51% of respondents say more money is allocated to IT security. Only 23% of respondents say an equal amount is allocated to IT security and physical security.

Figure 8. How does your organization allocate its IT and physical information security budget?



APPLYING THESE INSIGHTS TO SECURE YOUR ORGANIZATION.

- ✓ **Broaden the responsibilities of the CISO and CSO to include information in any form –** the paperless office may never happen so the risks that paper documents represent will not be going away either. Make document security an integral part of your information security program.

- ✓ **Ensure legislative and regulatory awareness and compliance is part of the CISO or CSO role –** a surprising number of respondents indicated poor awareness of some major pieces of legislation. Make sure whomever is responsible for compliance or information security, has the additional responsibility of being aware of and keeping compliant with all legislation and regulations – not just digital laws.

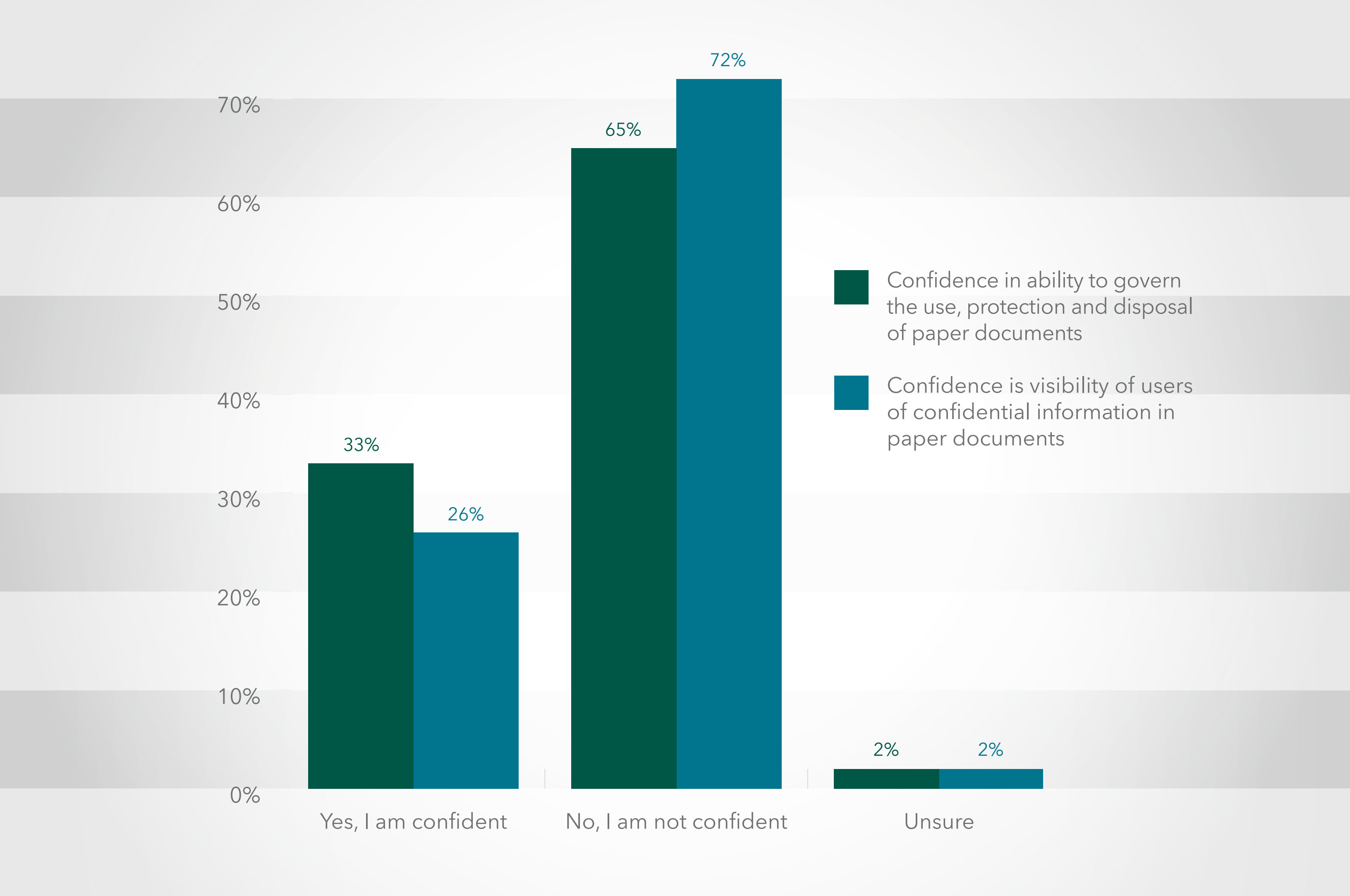
- ✓ **Engage with a document security partner –** compared to the costs of implementing and maintaining a cyber-security program, document security is an extremely affordable investment. And with 69% of reported incidents involving paper documents, this investment should be considered a priority. For the majority of respondents, they recognize this approach is more secure, convenient, and economical.

Reasons for the lack of security around confidential documents in the workplace.

The lack of policies and training for the secure disposal is having an effect on respondents' confidence in keeping confidential documents secure.

According to Figure 9, only one-third of respondents have confidence in their organizations' ability to govern the use, protection and disposal of paper documents. Fewer respondents (26%) have confidence in having visibility into what employees are doing with confidential documents.

Figure 9. How confident are you that your organization is able to protect paper documents?

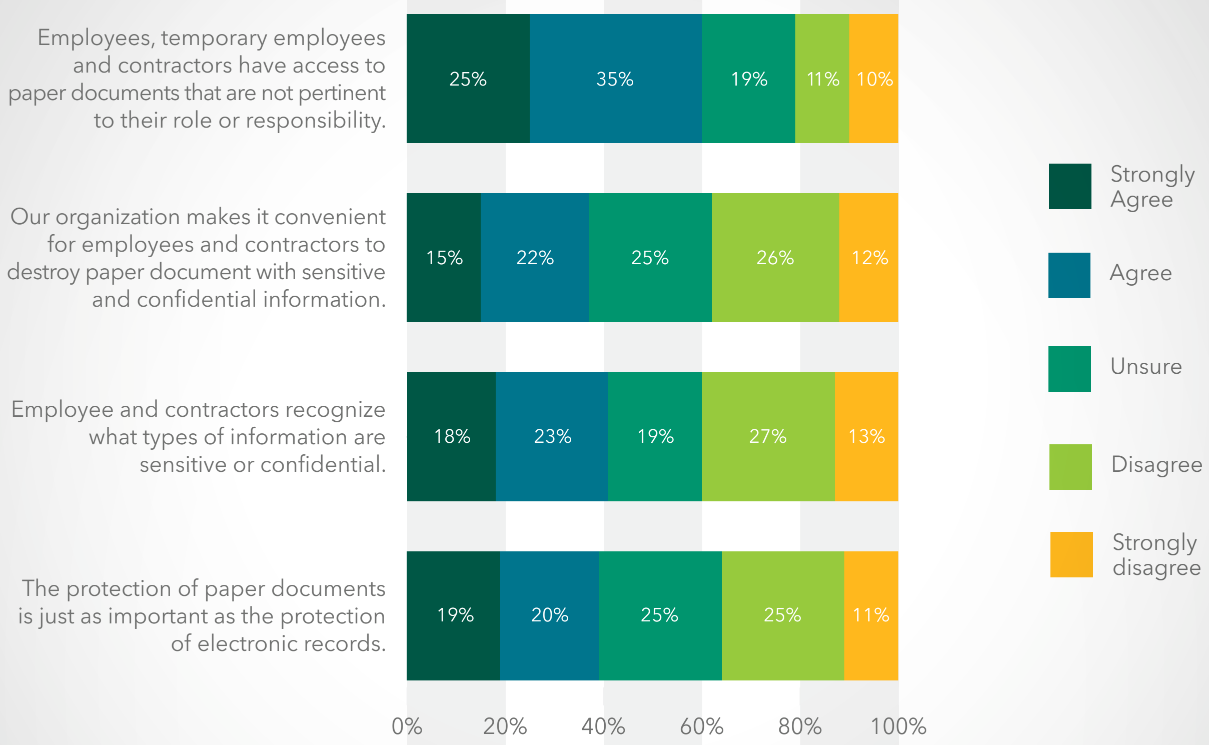


Organizations are unable to restrict employees' access to paper documents they should not see.

Figure 10 illustrates the workplace risks to confidential documents. Most respondents (61%) are unsure or disagree that the protection of paper documents is just as important as the protection of electronic records.

As a result, 60% of respondents strongly agree or agree that employees, temporary employees and contractors have access to paper documents that are not pertinent to their role or responsibility. Only 37% of respondents strongly agree or agree that it is convenient for employees and contractors to destroy paper documents with sensitive and confidential information. The fact that only 41% of respondents agree employees and contractors recognize the types of information that are sensitive or confidential demonstrates the lack of training in organizations.

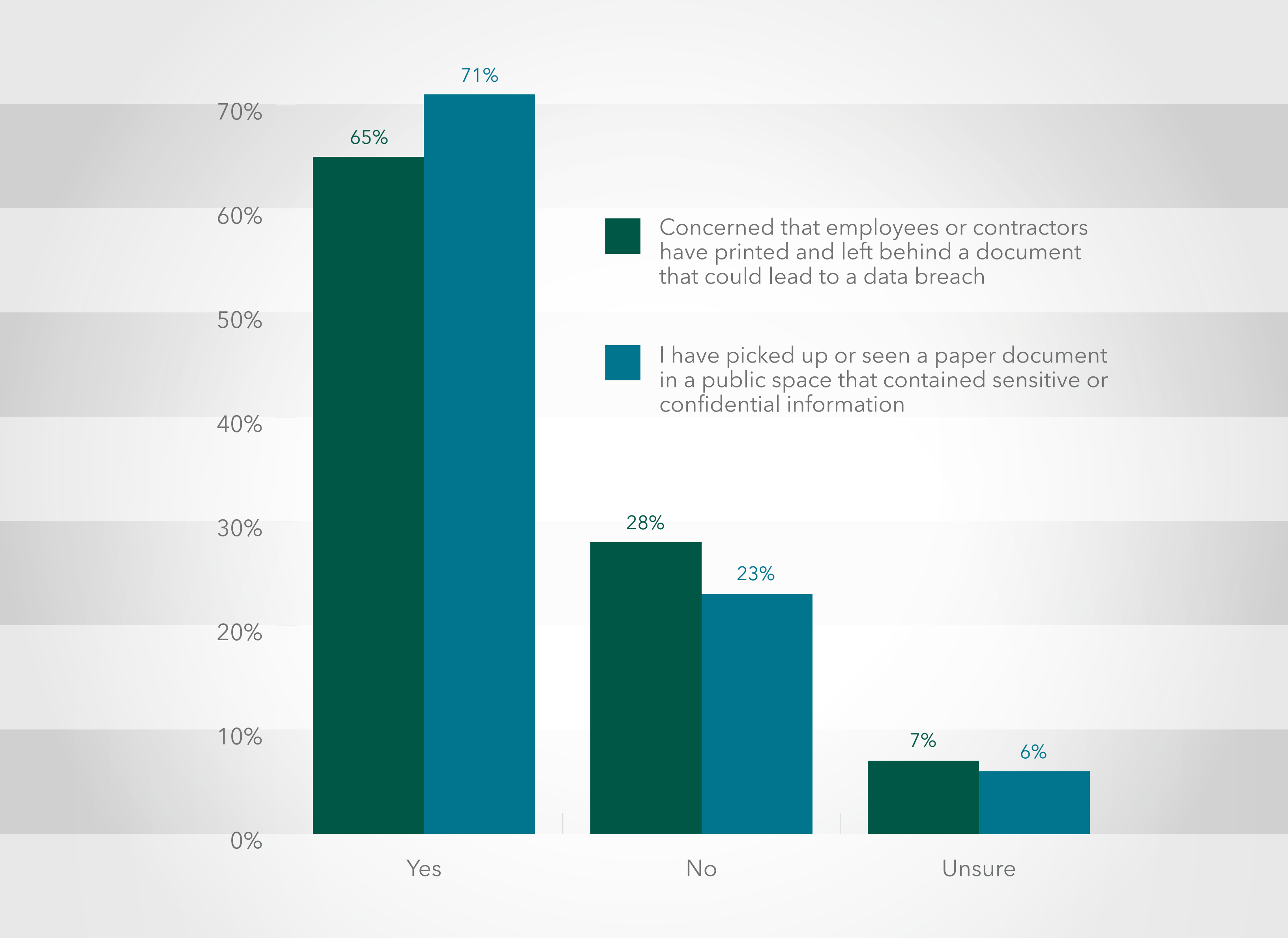
Figure 10. Perceptions about the insecurity of confidential documents. *Strongly Agree, Agree, Unsure, Disagree and Strongly Disagree responses shown.*



Confidential documents are left in plain sight.

As shown in Figure 11, 65% of respondents are concerned that employees or contractors have printed and left behind a document that could lead to a data breach. Even more respondents (71%) admit they have picked up or seen a paper document in a public space that contained sensitive or confidential information.

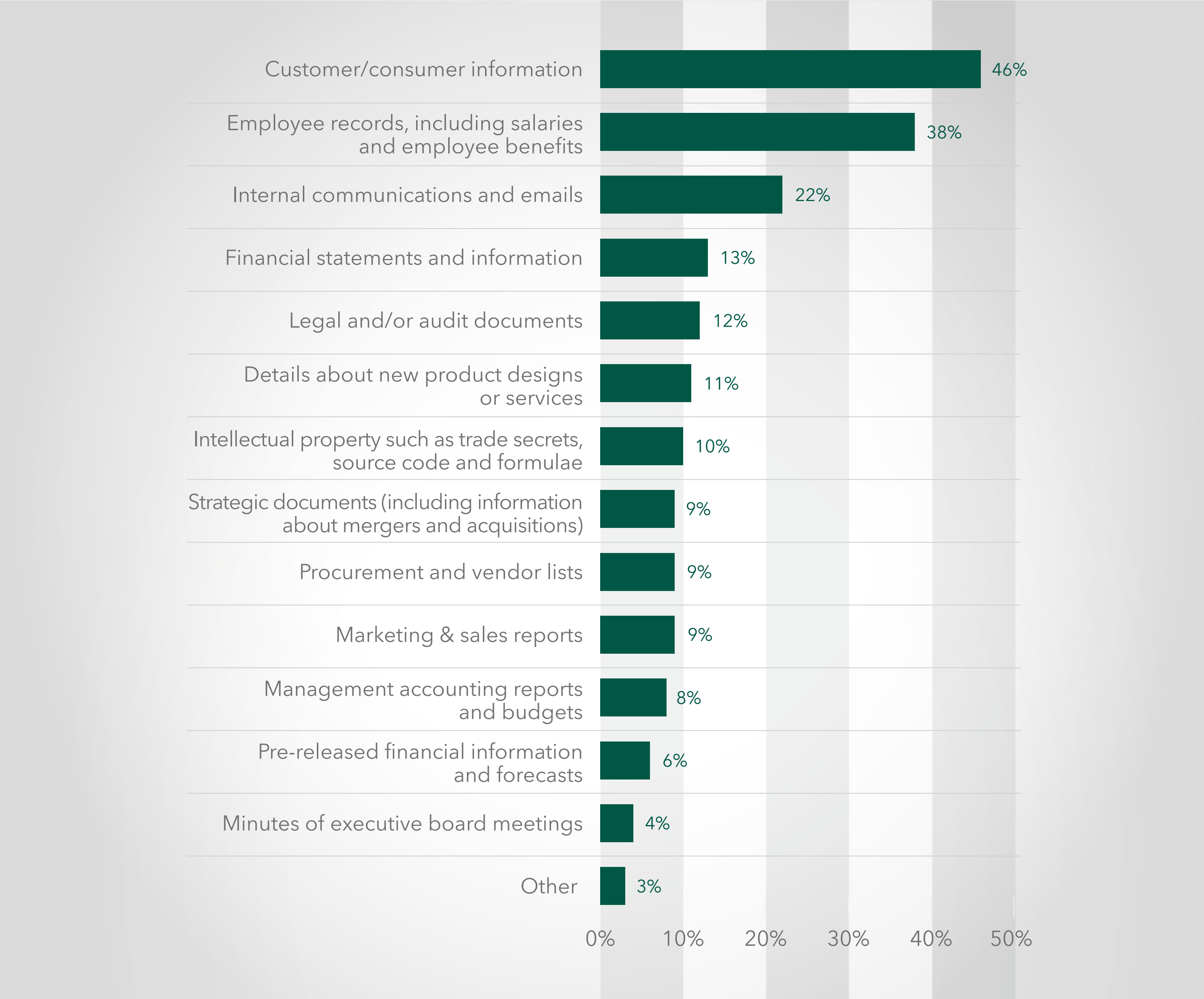
Figure 11. Risky practices in the workplace.



What do employees know about data that needs to be safeguarded?

Respondents were asked what they think their employees consider information that is most at risk. As shown in Figure 12, the top two information types are customer/consumer information (46% of respondents) and employee records (38% of respondents).

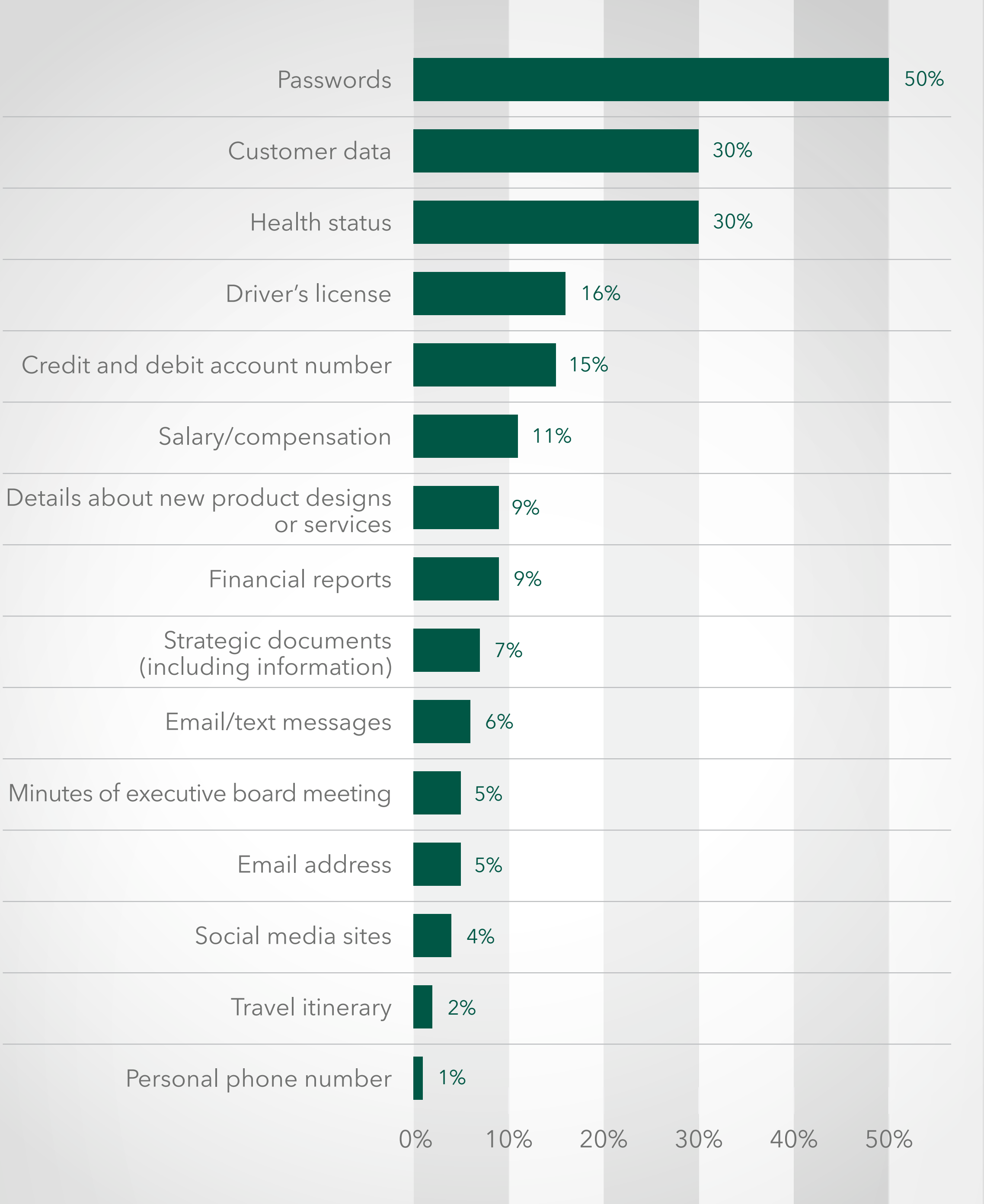
Figure 12. Risky practices in the workplace.



What data elements do employees consider most confidential.

The number one data element most at risk, as shown in Figure 13, is the password (50% of respondents). This is followed by customer data and health status (30% of respondents).

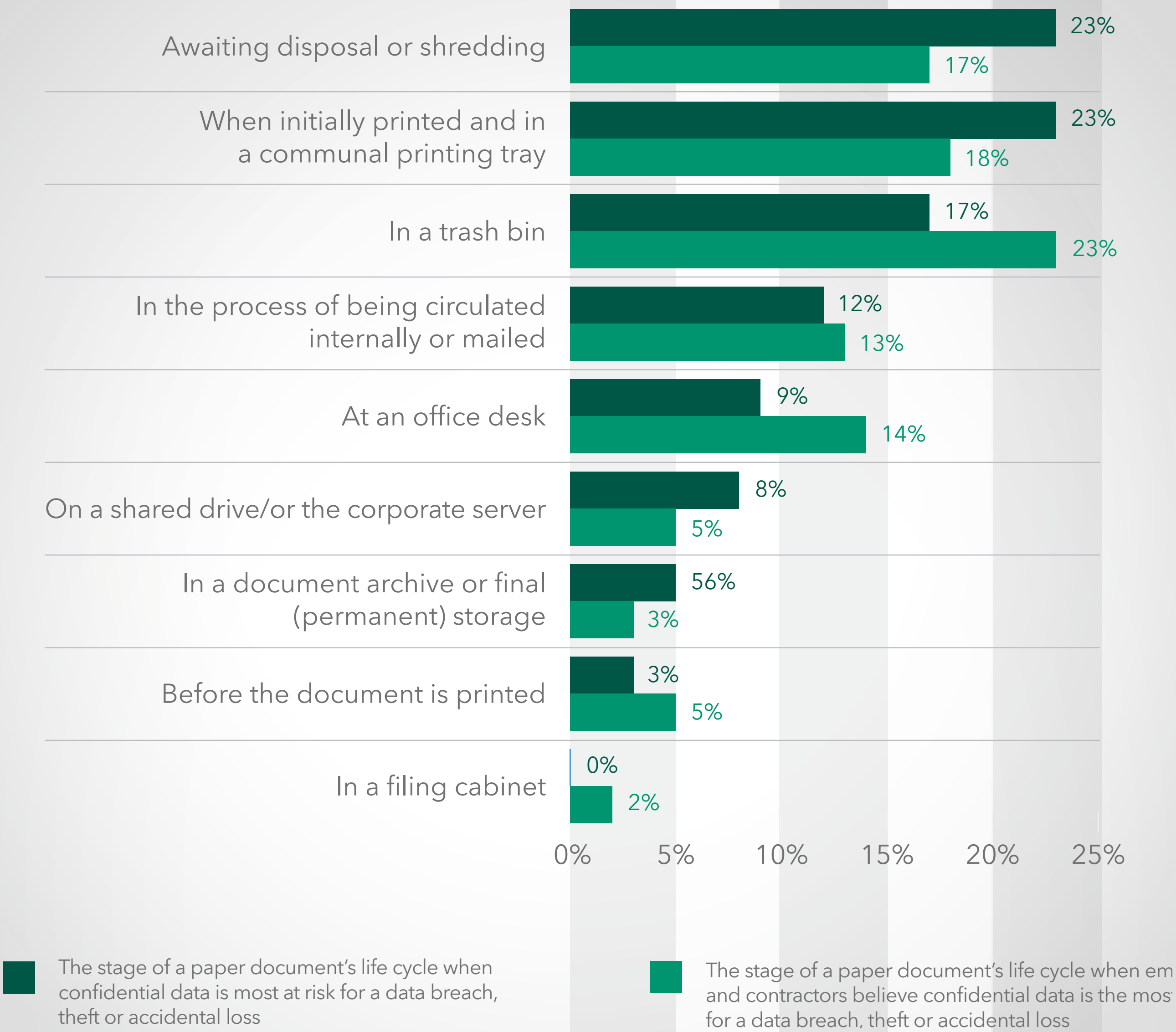
Figure 13. Data elements employees consider most confidential and at risk.



Do employees and contractors understand when paper documents are at risk for a data breach?

According to Figure 14, there is a gap between what respondents believe is the riskiest period in the document's life cycle and what they believe is employees' awareness about the risk. Specifically, 23% of respondents believe the greatest risk is when the document is awaiting disposal or shredding or when initially printed and in a communal printing tray. 23% of respondents say employees believe the risk is when the documents are in a trash bin.

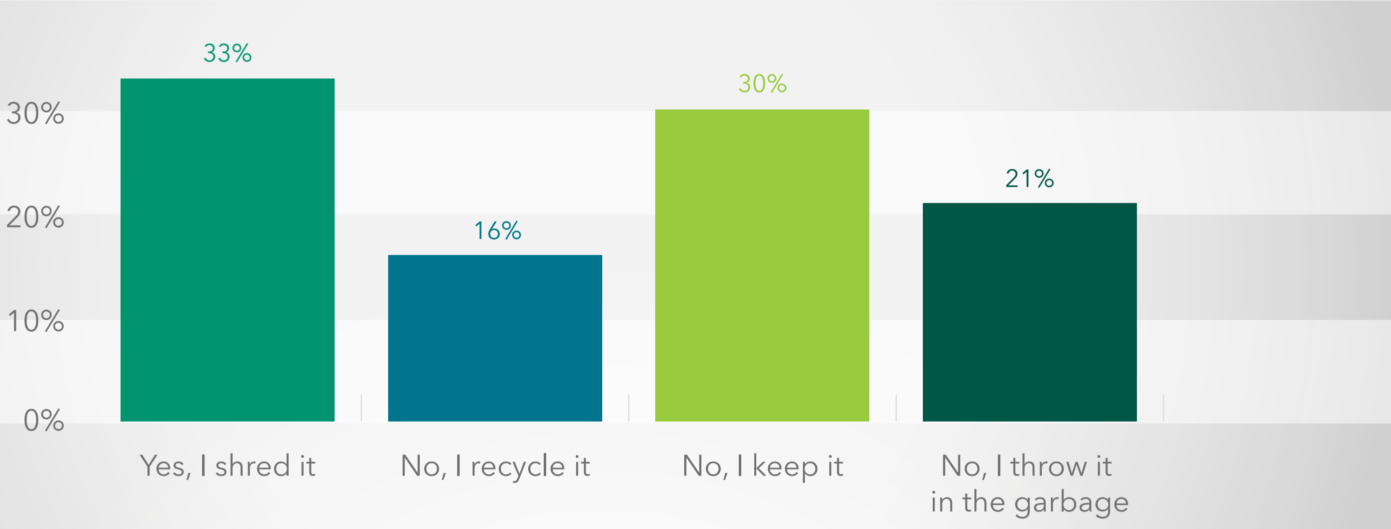
Figure 14. At what stage of a paper document's life cycle considered most at risk for a data breach?



More than half (51% of respondents) say they either keep the document or throw it in the garbage.

Only 33% of respondents say they shred the document after reviewing it, as shown in Figure 15.

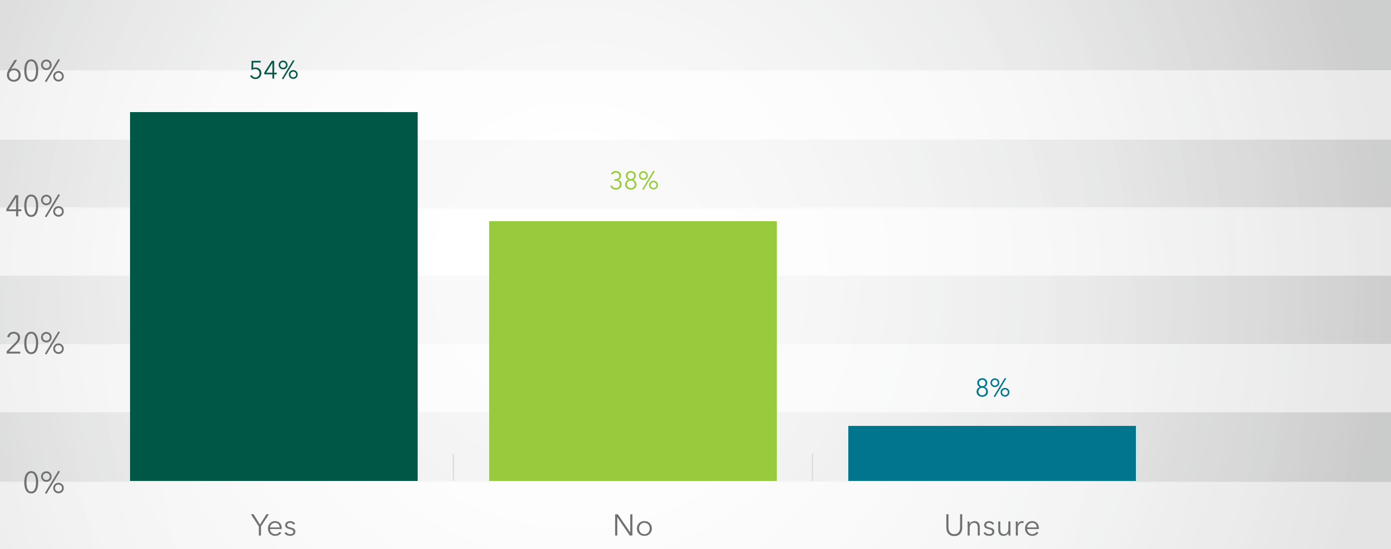
Figure 15. Do you shred paper documents after you have reviewed them?



Phishing emails and social engineering scams are prevalent in the workplace.

According to Figure 16, 54% have been the target of these attacks. However, 61% of respondents did not report the incident to their supervisor.

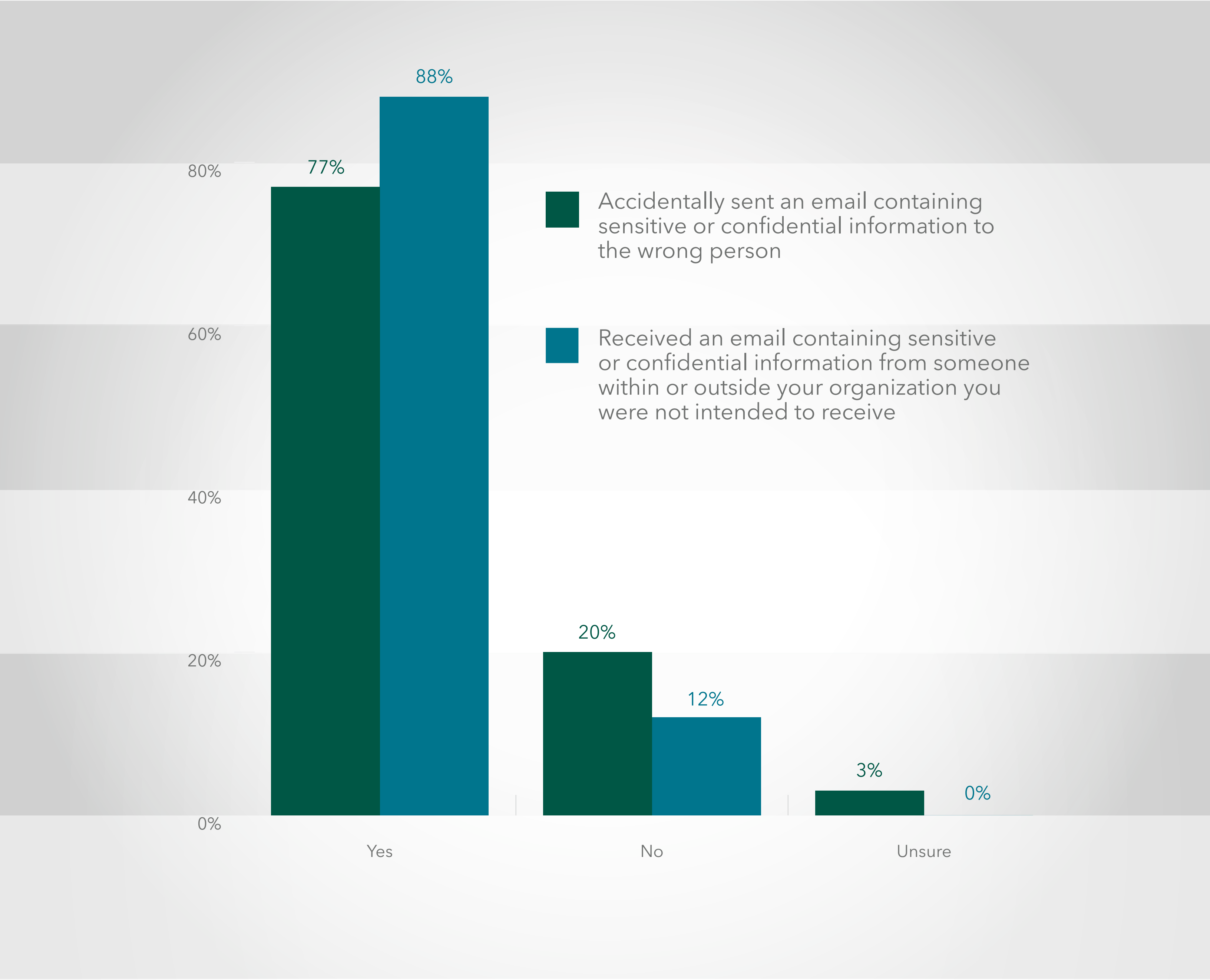
Figure 16. Have you been targeted by a phishing email or social engineering scam at work?



Sensitive or confidential information is exposed because of sending and receiving emails not intended for the recipient.

As shown in Figure 17, 77% of respondents admit to sending emails containing sensitive or confidential information to the wrong person. 88% of respondents say they have received such emails.

Figure 17. Risky email practices.



APPLYING THESE INSIGHTS TO SECURE YOUR ORGANIZATION.

Integrate education into employee onboarding – whoever is responsible for information security onboarding and training programs should include document security as well. Additionally, by making it part of your continuing education training and performance reviews, you begin to create a culture of information security.

Implement workplace privacy policies – there are basic actions every employee can take to reduce the risk of a breach: locking desks and filing cabinets, securing access to on-site storage. But you can augment that security by implementing privacy guidelines like a *Clean Desk* policy and a *Shred-it All* policy.

Broaden everyone's definition of confidential – less than half of respondents considered consumer/customer information as most confidential and at risk. Financial and legal documents were considered as most confidential and at risk by only 13% and 12% of respondents respectively. The truth is **all** of the documents in Figure 12 should be considered confidential and should be protected.

Provide a document management process – some employees think documents are most at risk when they are waiting for disposal, others think it is when the document is sitting on the printer. In fact, documents are at risk throughout their life cycle. The best way to protect them is to implement a *Document Management* policy that describes how to keep confidential documents secure at all times.

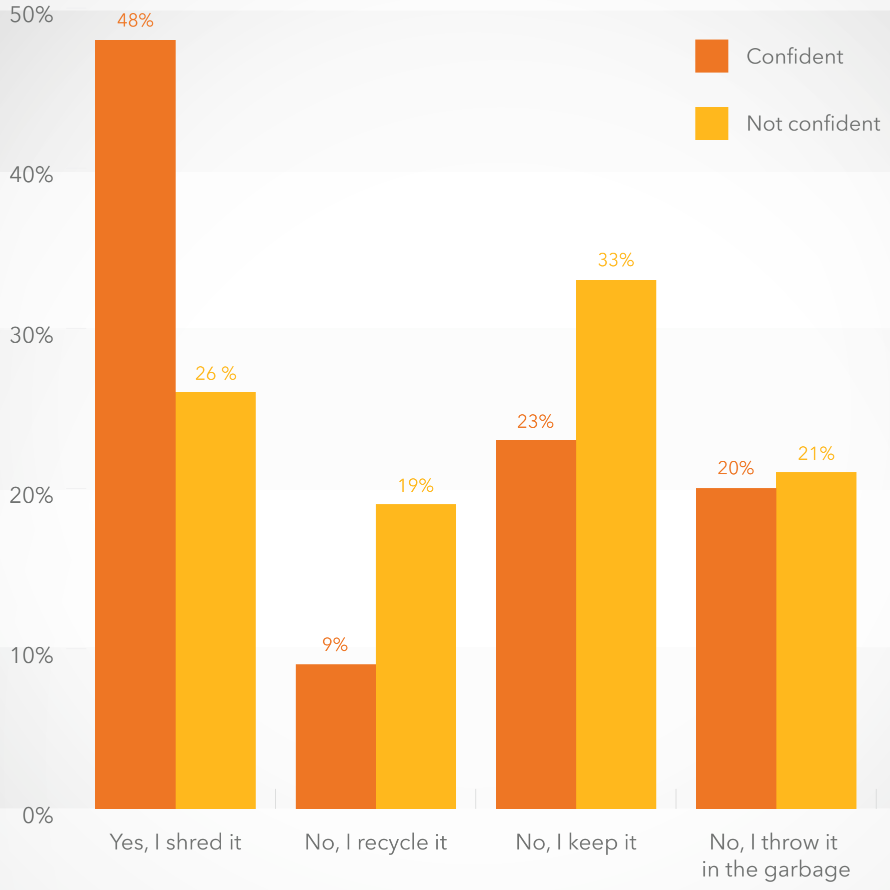
The practices of organizations that are more confident in their ability to protect documents and devices.

In this section, we present a special analysis of those respondents who self-reported that they are confident in their organizations ability to govern the use, protection and disposal of paper documents (33% of respondents).

An important indicator of confidence is that more of these respondents are shredding documents following their review.

According to Figure 18, almost half of respondents (48%) are shredding. However, this is still low because it should be 100%.

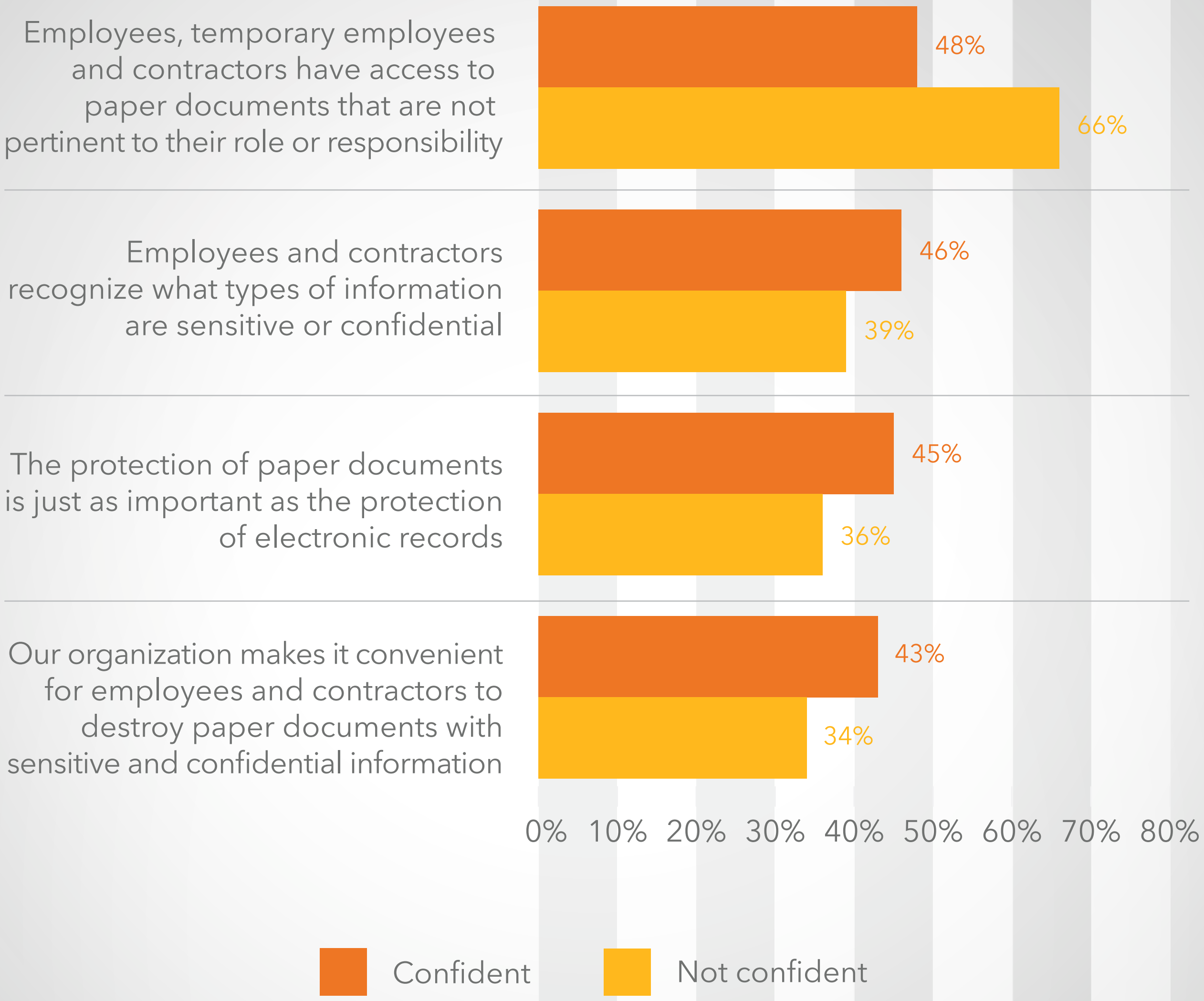
Figure 18. Do you shred paper documents after you have reviewed them?



In every case, confident respondents are more likely to believe their organizations are proactive in protecting documents.

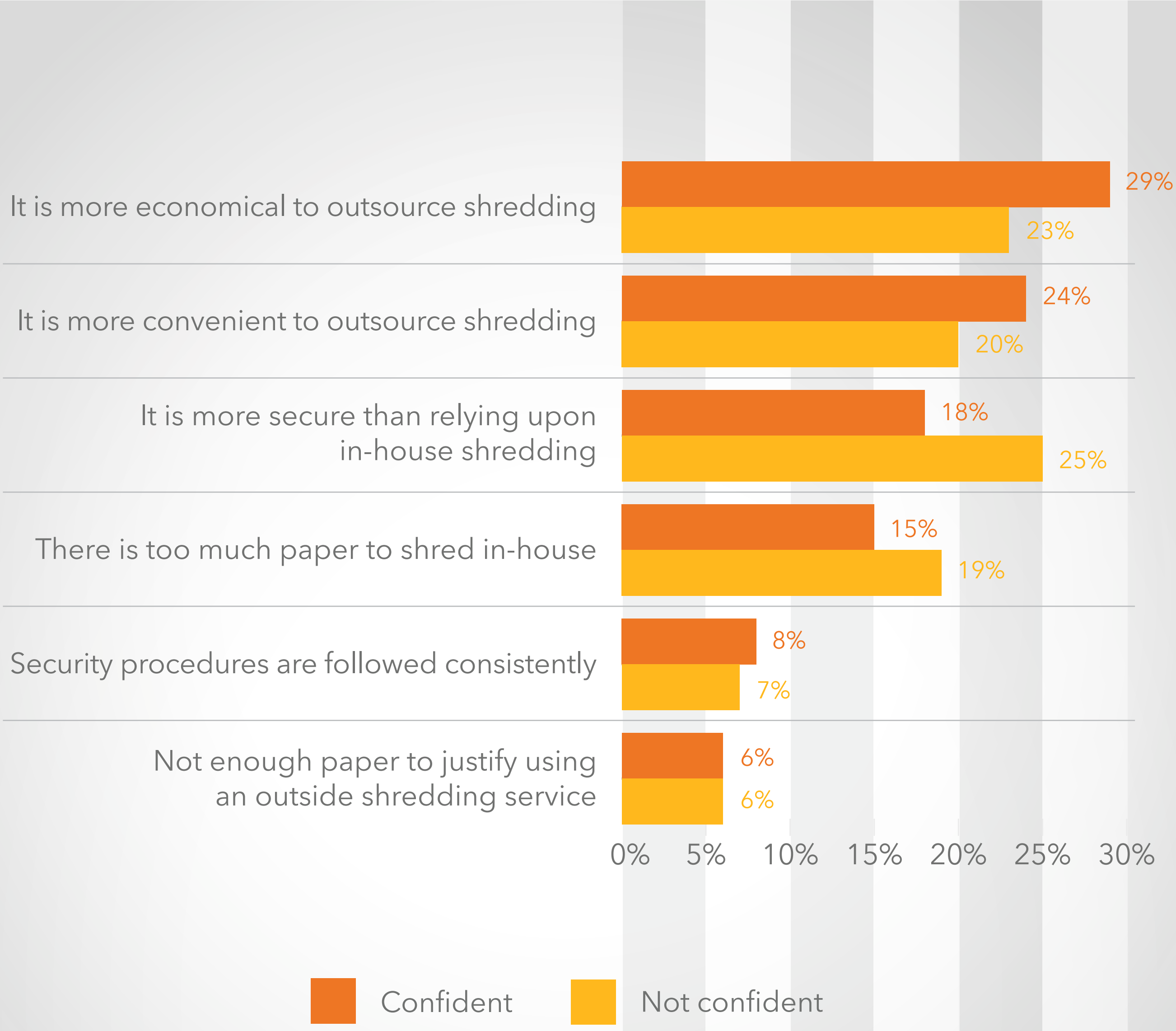
According to Figure 19, confident respondents are more likely to agree that access to paper documents not relevant is restricted, that employees and contractors understand what information is confidential, that it is important and that it is convenient to destroy documents.

Figure 19. Perceptions about the protection of paper documents.
Strongly Agree and Agree responses combined.



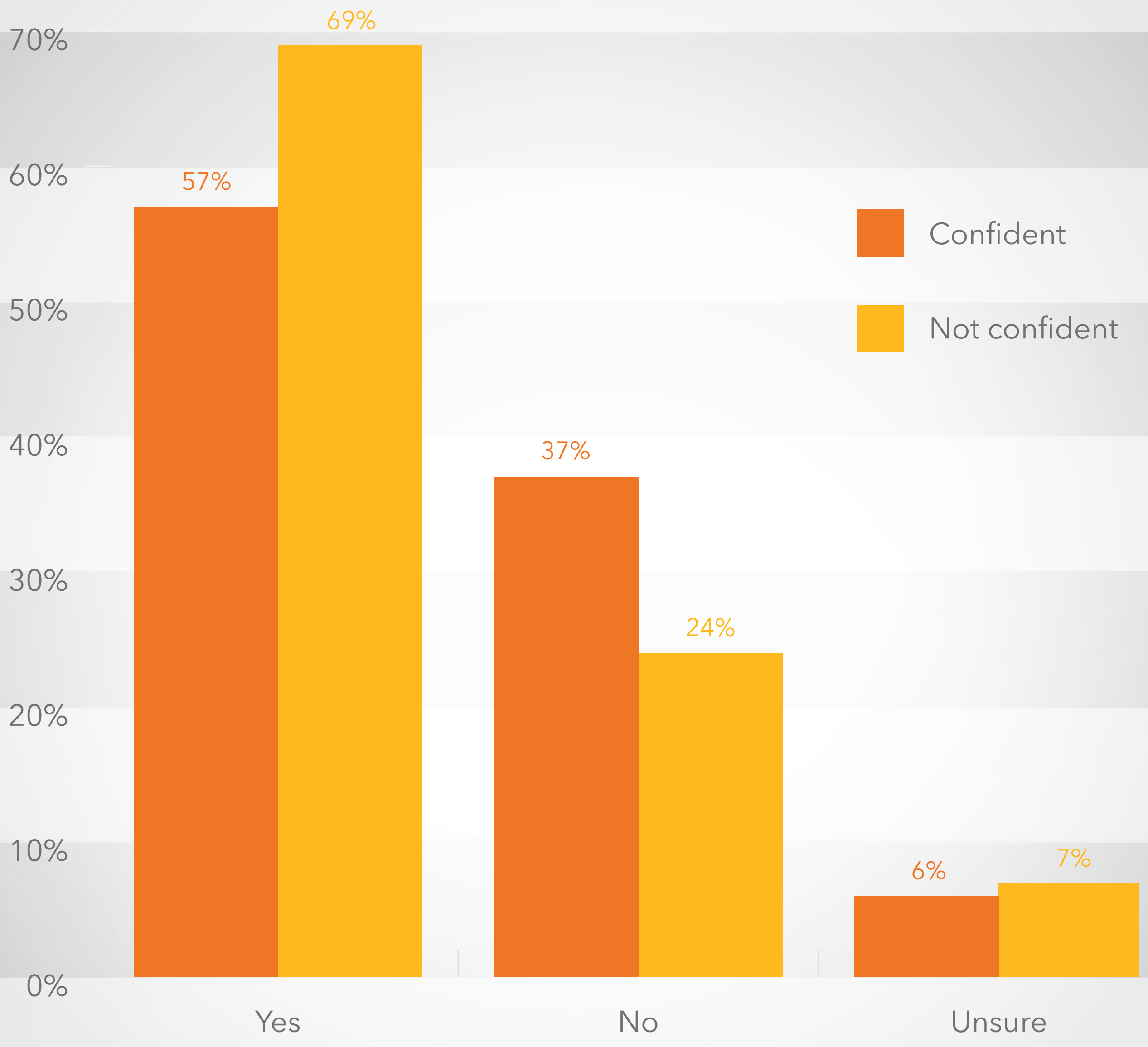
Confident respondents are using outside shredding services because it is economical and convenient, as shown in Figure 20.

Figure 20. Why does your organization use an outside shredding service?



Confident respondents are less concerned that employees or contractors have printed and left behind a document that could lead to a data breach, as shown in Figure 21.

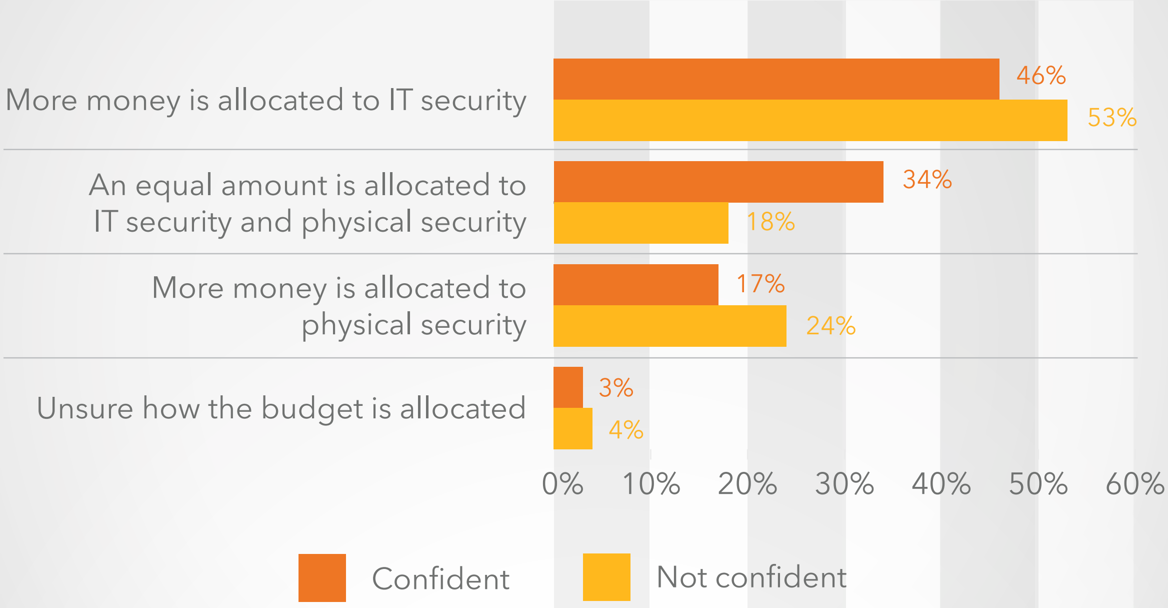
Figure 21. Are you concerned that employees or contractors have printed and left behind a document that could lead to a data breach?



Bigger budgets build confidence.

The average budget for organizations that have confident respondents is $3.26 million. In contrast, the not confident group's average budget is $2.31 million. As shown in Figure 22, the confident group has more money allocated to physical security.

Figure 22. How does your organization allocate its IT and physical information security budget?



APPLYING THESE INSIGHTS TO SECURE YOUR ORGANIZATION.

Restrict access to paper documents – there is really no reason why employees should have access to every piece of paper within an organization. Not only does unrestricted access increase the risk for an information breach, but it also makes version control, storage and document filing more difficult.

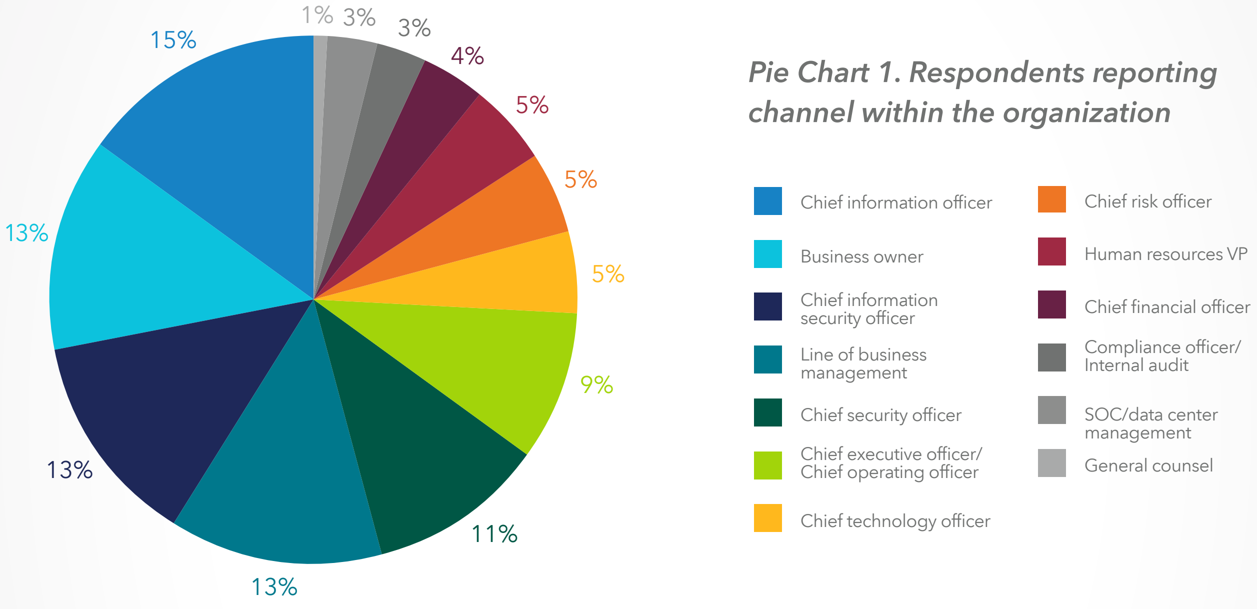
Make an investment in document security – compared to the costs of implementing and maintaining a cyber-security program, document security is an extremely affordable investment. And with 69% of reported incidents involving paper documents, this investment should be considered a priority.

METHODS

A sampling frame of 15,910 individuals in IT security and non-IT positions located in North America and who are knowledgeable about their organization's strategy for the protection of confidential and sensitive information were selected as participants in the research. Table 1 shows that there were 706 total returned surveys. Screening and reliability checks led to the removal of 56 surveys. Our final sample consisted of 650 surveys, a 4.1% response.

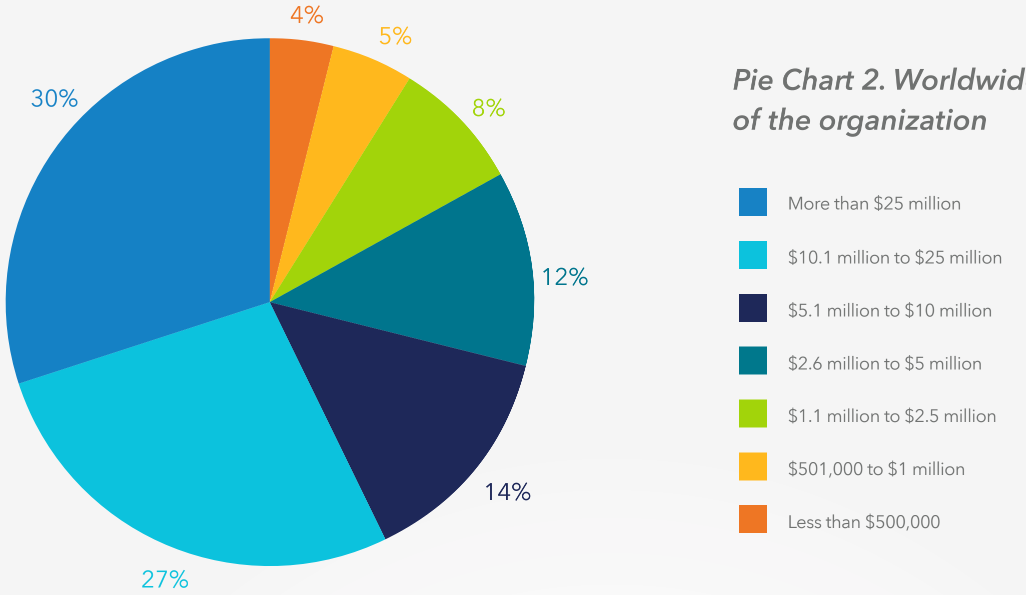
TABLE 1. SAMPLE RESPONSE	Freq	Pct %
Total sampling frame	15,910	100.0%
Total returns	706	4.4%
Rejected surveys	56	0.4%
Final sample, North America	650	4.1%

As shown in Pie Chart 1, 15% of respondents report to the chief information officer, 13% of respondents report to the business owner, 13% of respondents report to the chief information security officer, 13% of respondents report to line of business management and 11% of respondents report to the chief security officer.

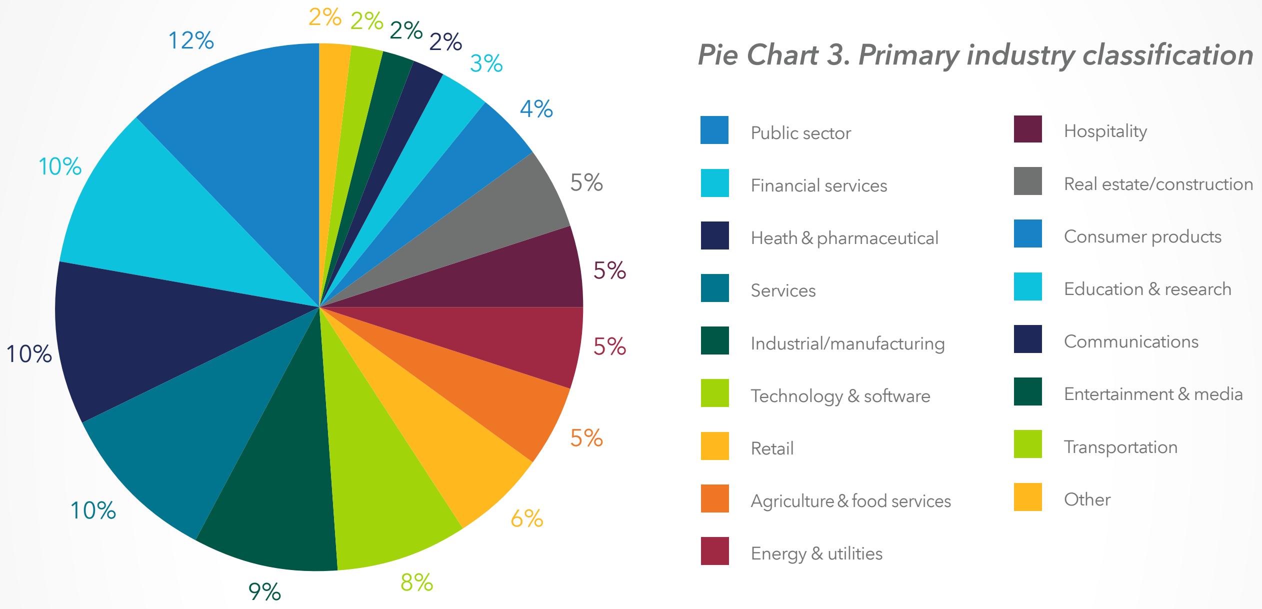


Pie Chart 1. Respondents reporting channel within the organization

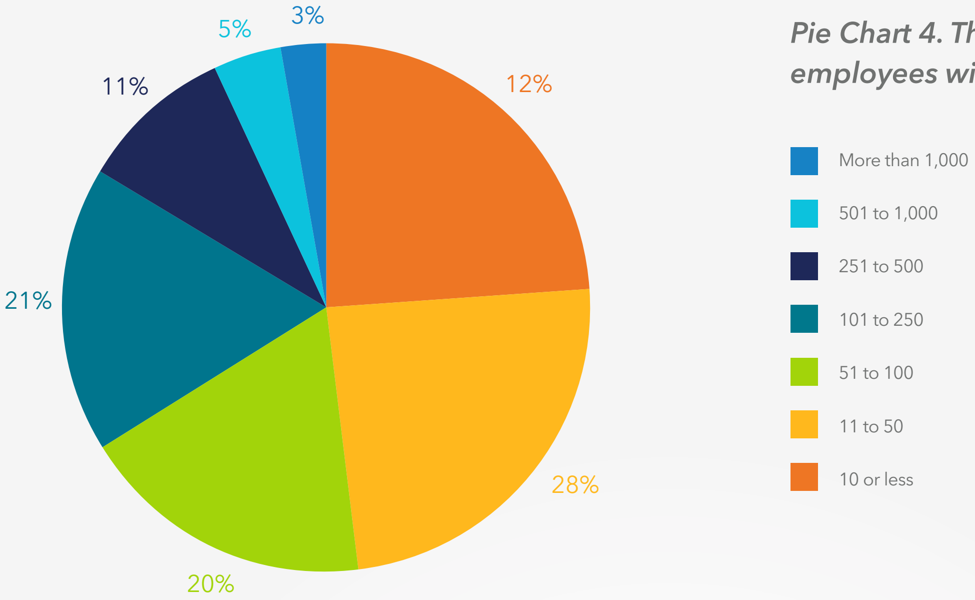
According to Pie Chart 2, more than half of the respondents (57%) are from organizations with a worldwide revenue of over $10 million.


Pie Chart 2. Worldwide revenue of the organization

Pie Chart 3 reports the industry classification of respondents' organizations. The largest industry classification is public sector (12% of respondents), followed by financial services (10% of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals, and services, each at 10% of respondents.


Pie Chart 3. Primary industry classification

According to Pie Chart 4, more than half of the respondents (60%) are from organizations with a headcount of over 50 employees.



Pie Chart 4. The number of employees within the organization

Caveats to this study.

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals in IT and non-IT positions, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are knowledgeable about their organization's strategy for the protection of confidential and sensitive information. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

IMPROVING YOUR ORGANIZATION'S DOCUMENT SECURITY IN SIX EASY STEPS

Document security is more than paper shredding; it is an end-to-end approach to document management, from creation to destruction, that keeps your confidential information safe and secure over its entire life cycle.

Here is what you need to do in order to build an effective document security program in your organization:

1. Get an information security risk assessment – knowing what the risks are and where to find them is an essential first step in any document security program. An on-site risk assessment helps identify what practices and procedures are putting your organization at risk and provides recommendations about how to mitigate them.

2. Provide awareness training – well-informed, trained employees can reduce your risk almost immediately. Create a culture of information security by teaching staff what to watch out for and what they can do to reduce your risk.

3. Implement workplace privacy policies – policies and practices designed to protect paper documents, specifically, will help maintain your information security when confidential information is found in paper form. Implementing *Document Management* policies, *Clean Desk* policies, and *Shred-it® All* policies are good examples of effective workplace practices.

4. Deploy secure, locked consoles throughout the workplace – when employees have to choose between what should be trashed, recycled, or shredded, they invariably make mistakes that could lead to an information breach. Make it easy on them by replacing trash cans and recycling bins with tamper-proof consoles and directing them to put ALL documents in one secure place.

5. Destroy your documents on a regular schedule – make sure you engage with a reputable document destruction company who will collect, destroy and securely recycle your unused documents. Make sure they employ a *secure chain of custody* at every touch point and that they issue a *Certificate of Destruction* after every service to prove your compliance with required privacy legislation.

6. Do periodic clear-outs – no matter how hard you try, paper will still pile up. Archival records in the storage room and filing cabinets are the two biggest culprits. But the document destruction company you hire for regular service will also come to your offices periodically to clear-out the overflow, decluttering the office and further reducing your risks.

As this report highlights, paper documents pose real risks to your overall information security.

Assigning organizational responsibility to ensure document security is part of your overall information security program is essential. Implementing awareness training and adopting workplace privacy policies are also important steps your organization can easily take.

Additionally, consider engaging a partner who can help you build and maintain an effective document security program. As the research shows, this is seen as a best practice by the majority of the survey respondents. Shred-it has the expertise and experience to be part of the solution, and is committed to helping protect and safeguard data, reputation and businesses.

Information has never been more valuable. And the need to protect it? Never more important.

Choose the information security partner who can help you meet the growing information security challenges facing your organization. With industry-leading information security services, Shred-it helps protect your reputation, your revenue, and your business.

Security Expertise

With 30 years of destruction expertise and an end-to-end secure chain of custody, our primary focus on document security ensures your confidential information remains confidential.

Service Reliability

Whether you are a large-scale national enterprise or one of thousands of small businesses, you can put the power of the largest shredding fleet and the largest service footprint in North America to work for you.

Customer Experience

From a range of self-service options and customizable destruction solutions to responsive, dedicated, customer service support, Shred-it is 100% committed to your protection.

We protect what matters.

Learn more about information security and how Shred-it can protect your organization at **shredit.com** or call **800-697-4733** today.

Sponsored by Shred-it, this research reveals the inadequacies in organizations' policies regarding the protection of confidential documents in the workplace. Ponemon Institute surveyed 650 individuals who work in both IT security and non-IT positions in North American organizations. All respondents are knowledgeable about their organization's strategy for the protection of confidential and sensitive information.

Ponemon Institute: Advancing Responsible Information Management. Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations. We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.