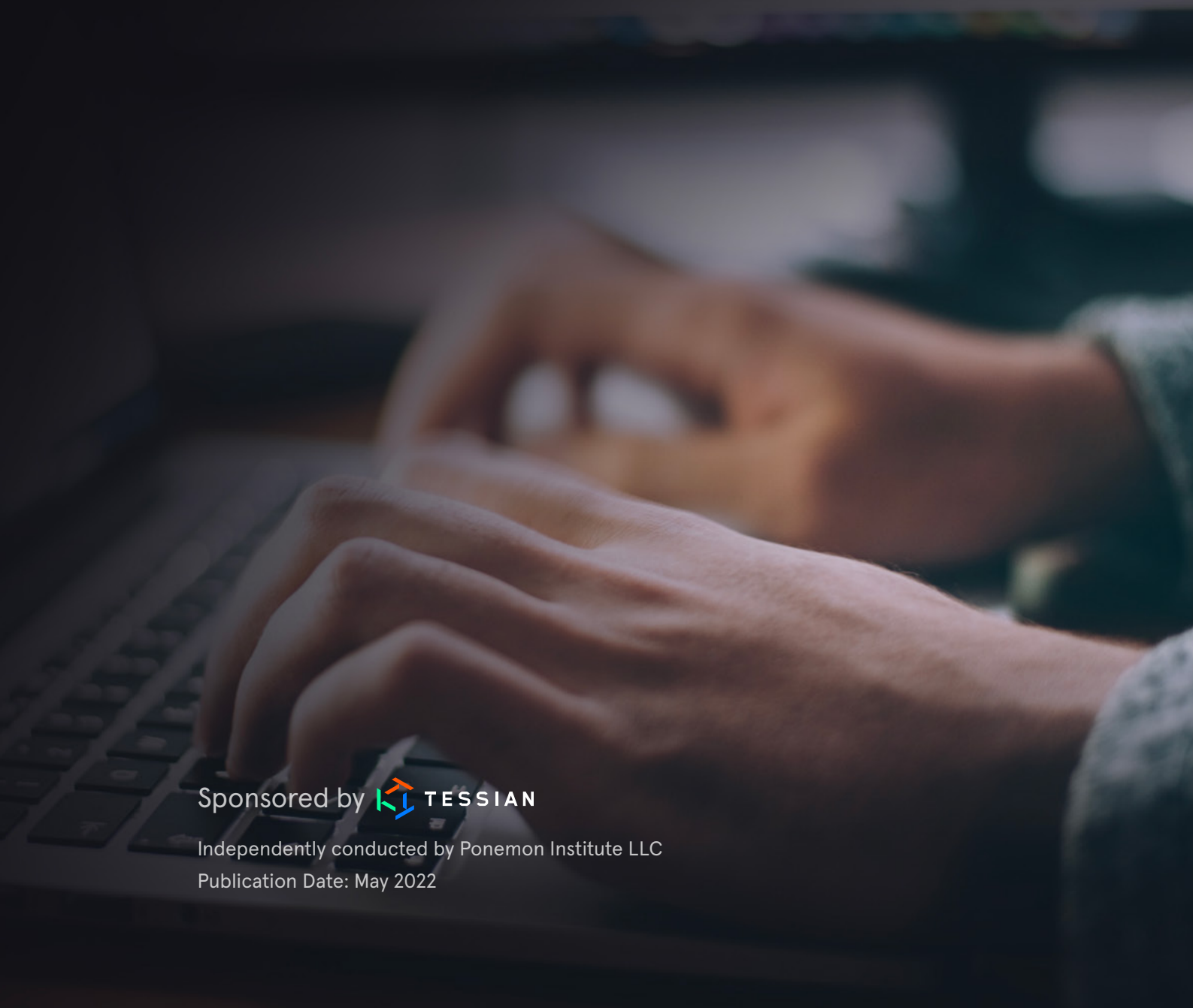
Ponemon INSTITUTE

# Email Data Loss Prevention: The Rising Need for Behavioral Intelligence



Sponsored by TESSIAN

Independently conducted by Ponemon Institute LLC
Publication Date: May 2022

**Email Data Loss Prevention:**
**The Rising Need for Behavioral Intelligence**
Prepared by Ponemon Institute, May 2022

## Part 1. Introduction

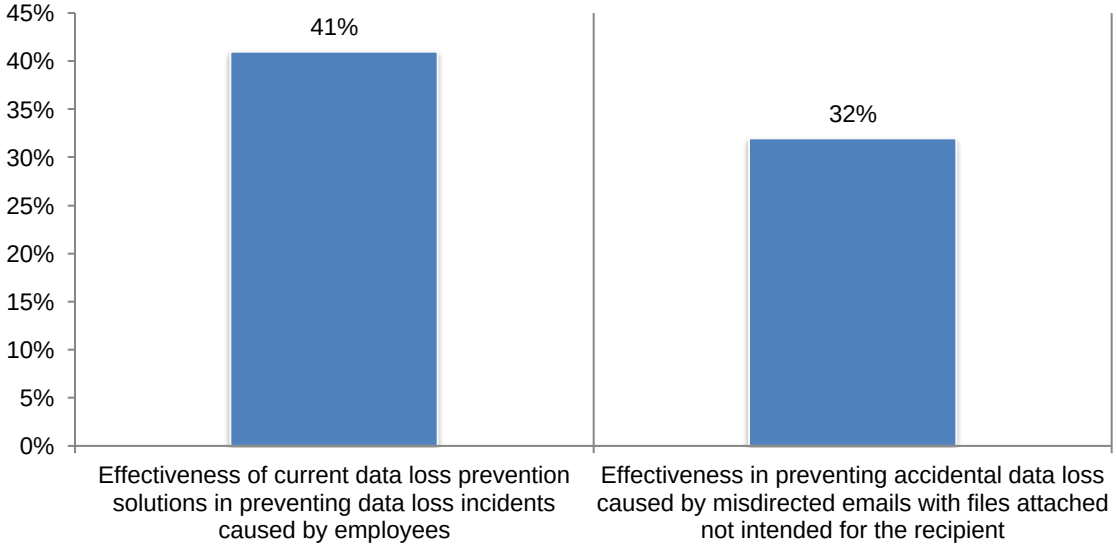
The purpose of this study is to learn what practices and technologies are being used to reduce one of the most serious risks to an organization's sensitive and confidential data. The study finds that email is the top medium for data loss and the primary pathways are employees' accidental and negligent data exfiltration through email. According to the research, 59 percent of respondents say their organizations experienced data loss and exfiltration that involved a negligent employee or an employee accidentally sending an email to an unintended recipient. On average, organizations represented in this research had 25 of these incidents each month.

To reduce these risks, organizations should consider technologies that leverage machine learning and behavioral capabilities. This approach enables organizations to proactively prevent data loss vulnerabilities so organizations can stop email data loss and exfiltration before they happen. Thirty-six percent of respondents say their organizations use behavior-based machine learning and artificial intelligence technology. Seventy-seven percent of these respondents report that it is very effective.

Sponsored by Tessian, Ponemon Institute surveyed 614 IT and IT security practitioners who are involved in the use of technologies that address the risks created by employees' negligent email practices and insider threats. They are also familiar with their organizations' data loss protection (DLP) solutions.

**Current solutions and efforts to minimize risks caused by employees' misuse of emails are ineffective.** Respondents were asked to rate the effectiveness of their organizations' ability in preventing data loss and exfiltration caused by vulnerabilities in employees' use of emails on a scale of 1 = not effective to very effective = 10. Figure 1 shows the effective and very effective responses (7+ on the 10-point scale). Only 41 percent of respondents say their current data loss prevention solutions are effective or very effective in preventing data loss caused by misdirected emails. As one consequence of not having the right solutions, **only** 32 percent of respondents say their organizations are effective or very effective in preventing these incidents.

**Figure 1. Effectiveness in preventing data loss incidents caused by employees**
On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



**The following recommendations are based on the research findings.**

- **Data is most vulnerable in email.** Employee negligence when using email is the primary cause of data loss and exfiltration. According to the research, 65 percent of respondents say data is most vulnerable in emails. In the allocation of resources, organizations should consider technologies that reduce risk in this medium. On average, enterprises have 13 full-time IT and IT security personnel assigned to securing sensitive and confidential data in employees' emails.

- **Organizations should assess the ability of their current technologies to address employee negligence risks related to email.** Forty percent of respondents say email data loss and exfiltration incidents were due to employee negligence or by accident. Additionally, 27 percent of respondents say it was due to a malicious insider. As revealed in this research, many current email data loss technologies are not considered effective in mitigating these risks. Accordingly, organizations should consider investing in technologies that incorporate machine learning and artificial intelligence to understand data loss vulnerabilities through a behavioral intelligence approach.

- **Identify the highest risk functions in the organization.** According to respondents**,** the practices of the marketing and public relations functions are most likely to cause data loss and exfiltration (61 percent of respondents). Accordingly, organizations need to ensure they provide training that is tailored to how these functions handle sensitive and confidential information when emailing**.** As shown in this research, organizations are most concerned about data loss involving customer and consumer data, which is very often used by marketing and public relations as part of their work.

  Other high-risk functions are production and manufacturing (58 percent of respondents) and operations (57 percent of respondents). Far less likely to put data at risk are client services and relationship management functions (19 percent of respondents).

- **Despite the risk, many organizations do not have training and awareness programs with a focus on the sensitivity and confidentiality of data transmitted in employees' email.** Sixty-one percent of respondents say their organizations have training and awareness programs for employees and other stakeholders who have access to sensitive or confidential personal information. Only about half (54 percent of the 61 percent of respondents with programs) say the programs address the sensitivity and confidentiality of data in employees' emails.

- **Sensitive and confidential information are at risk because of the lack of visibility and the ability to detect employee negligence and errors.** Fifty-four percent of respondents say the primary barrier to securing sensitive data is the lack of visibility of sensitive data that is transferred from the network to personal email. Fifty-two percent of respondents say the greatest DLP challenges are the inability to detect anomalous employee data handling behaviors and the inability to identify legitimate data loss incidents.

- **On average, it takes 18 months to deploy and find value from the DLP solution.** Organizations spend an average of slightly more than a year (12.3 months) to complete deployment of the DLP solution and more than half a year (6.5 months) to realize the value of the solution. The length of time to deploy and realize value can affect the ability for organizations to achieve a more mature approach to preventing email-related compromises by employees.

- **The length of time spent in detecting and remediating email compromises puts sensitive and confidential data at risk.** According to the research, security and risk management teams spend an average of 72 hours to detect and remediate a data loss and

exfiltration incident caused by a malicious insider on email and an average of almost 48 hours to detect and remediate an incident caused by a negligent employee. This places a heavy burden on these teams who must triage and investigate these incidents and become unavailable to address other security issues and incidents.

**Other takeaways**

- **Regulatory non-compliance is the number one consequence of a data loss and exfiltration incident followed by a decline in reputation.** These top two consequences can be considered interrelated because non-compliance with regulations (57 percent of respondents) will impact an organization's reputation (52 percent of respondents). Regulatory non-compliance is considered to have the biggest impact on organizations' decision to increase the budget for DLP solutions.

- **Organizations consider end-user convenience very important.** Seventy-five percent of respondents say end-user convenience in DLP solutions is very important.

## Part 2. Key findings

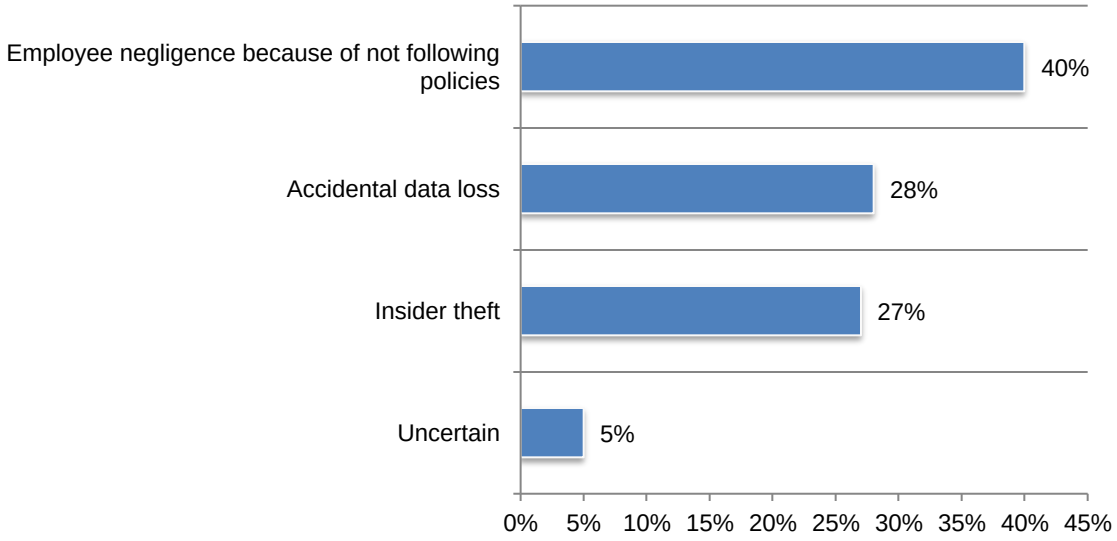
This section features an analysis of the research. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following themes.

- Risk of data loss due to email vulnerabilities
- The use of technologies and their effectiveness in preventing email data loss and exfiltration
- Barriers and capabilities that improve email data loss prevention

### Risk of data loss due to email vulnerabilities

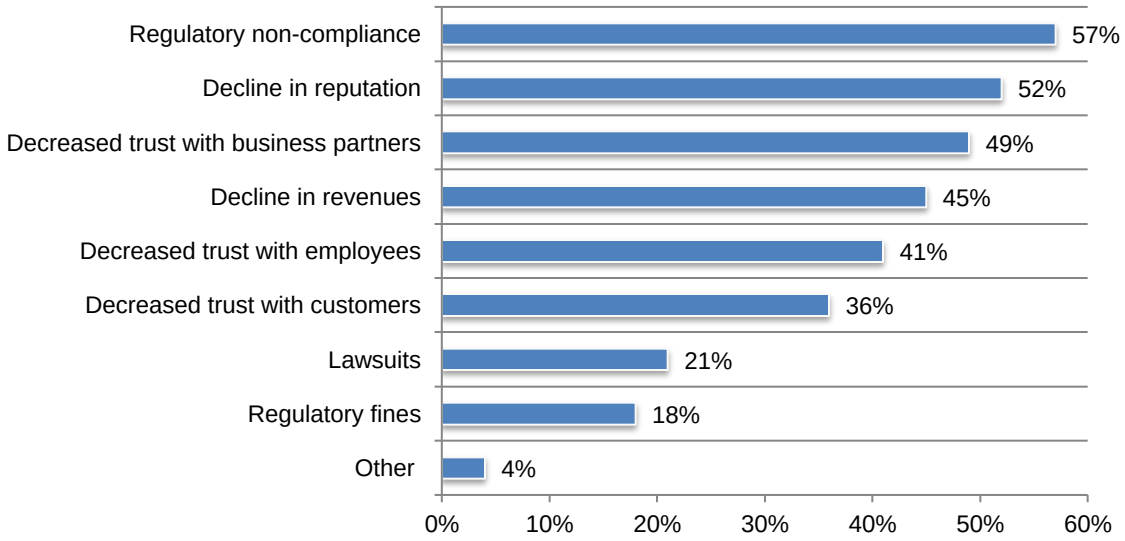
**Employee negligence is the primary cause of data loss and exfiltration.** In the past year, 59 percent of respondents say their organizations experienced data loss and exfiltration that involved employee negligence or an employee or by sending an email to an unintended recipient. On average, organizations had 25 of these incidents each month. According to Figure 1, 40 percent say it was due to employee negligence. Another 28 percent of respondents say it was due to an accident.

**Figure 2. How would you characterize the data loss and exfiltration?**
Only one choice permitted



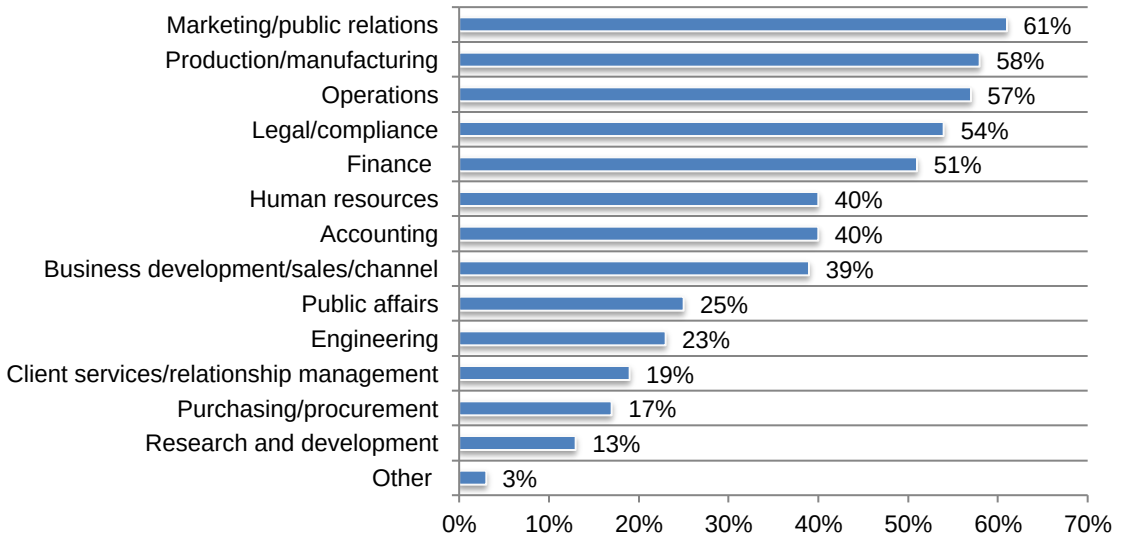
**Regulatory non-compliance is the number one consequence of a data loss incident.** Figure 3 presents the consequences from these incidents. The top two can be considered interrelated because non-compliance with regulations (57 percent of respondents) will impact an organization's reputation (52 percent of respondents).

**Figure 3. What were the consequences?**
More than one response permitted



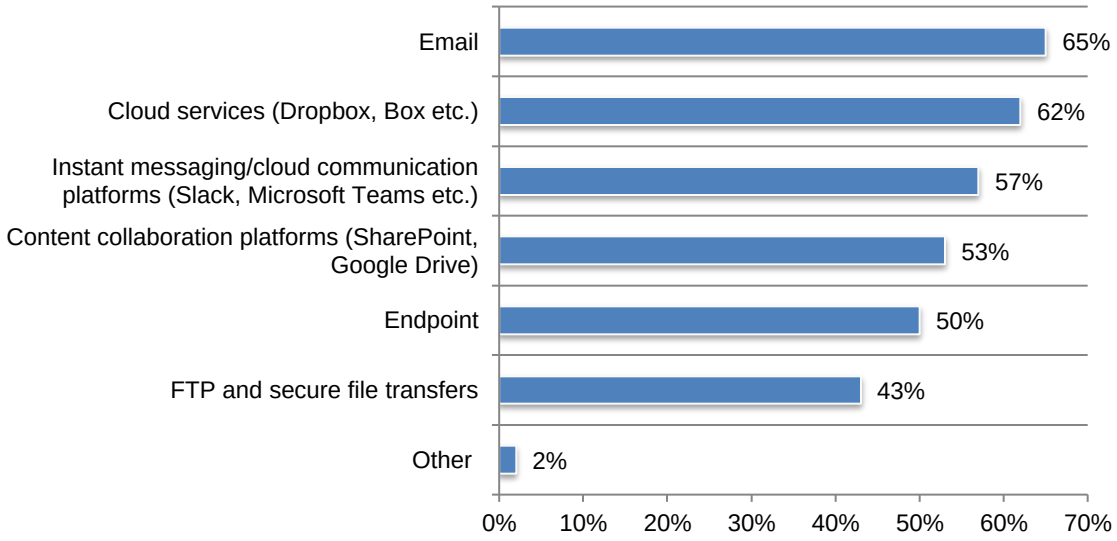

**Interestingly, the practices of the marketing and public relations functions are most likely to cause data loss and exfiltration (61 percent of respondents).** According to Figure 4, other top functions that are more likely to put data at risk are production and manufacturing (58 percent of respondents) and operations (57 percent of respondents). These are followed by legal/compliance (54 percent of respondents), finance (51 percent of respondents) and HR (40 percent of respondents). Organizations should assess those functions that are more negligent in the handling of data and ensure they receive a tailored training and awareness program on the risks of improper data handling.

**Figure 4. Who is more likely to put data at risk?**
More than one response permitted



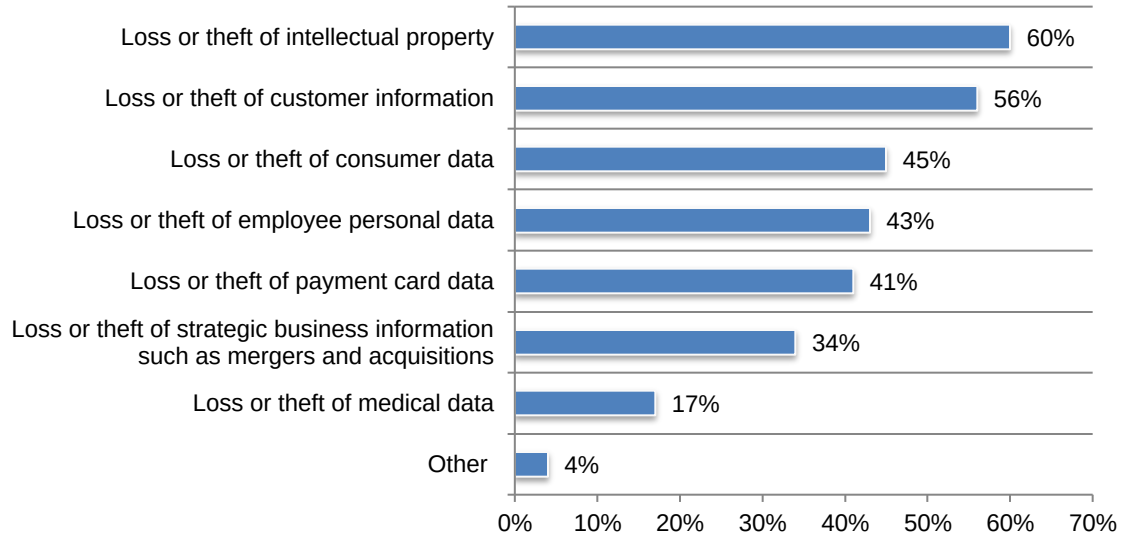
**Data is most vulnerable in emails.** As discussed previously, employee negligence when using email is the primary cause of data loss and exfiltration. According to Figure 5, 65 percent of respondents say email is the riskiest medium for data loss. In the allocation of resources organizations should consider DLP technologies that reduce risk in this medium as well as training and awareness programs to prevent employee negligence. On average, enterprises have 13 full-time IT & IT security personnel assigned to securing sensitive and confidential data in employees' email.

**Figure 5. The most common and the riskiest medium for the loss of sensitive data by employees**
More than one response permitted



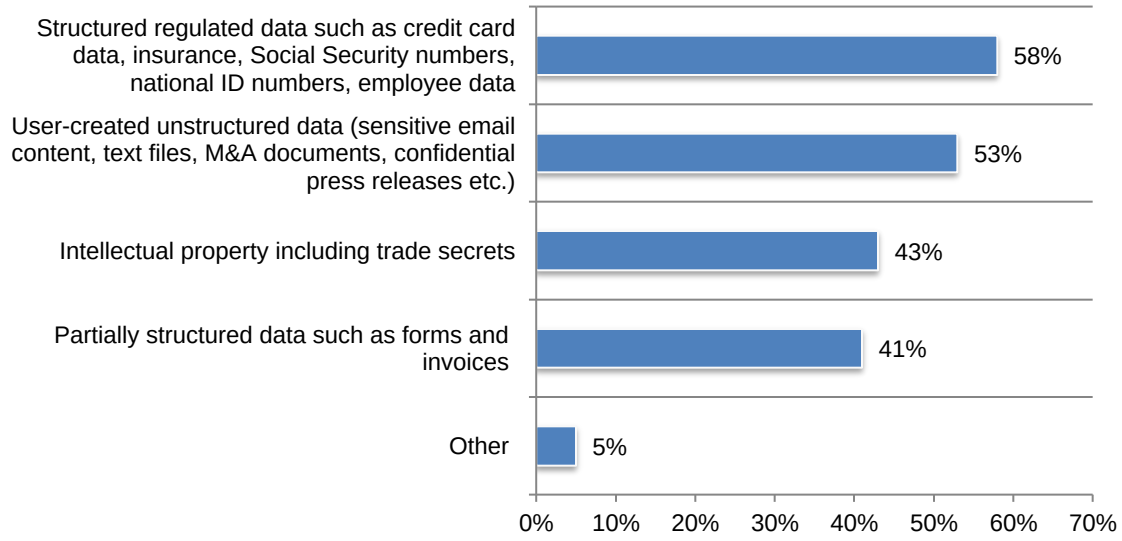
**The loss of customer and consumer data are top concerns.** According to Figure 6, while IP is the number one concern at 60 percent of respondents, customer and consumer data are close behind at 56 percent and 45 percent of respondents. As discussed previously, the functions that are considered to put data most at risk are marketing and PR and these functions are handling data that organizations are most concerned about—customer and consumer data.

**Figure 6. What types of data loss or exfiltration is your organization most concerned about?**



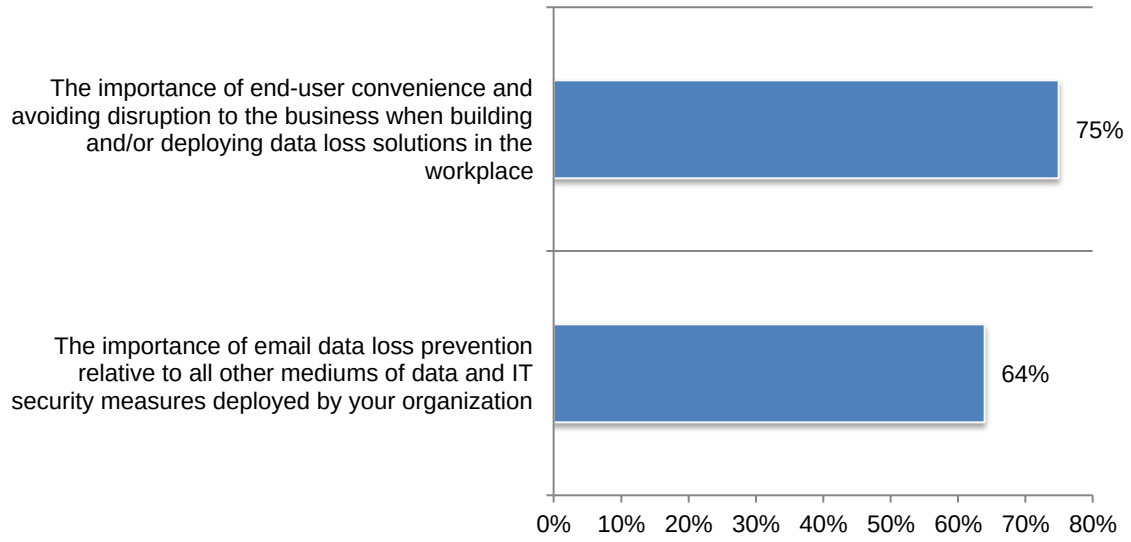
**Regulated data is the most difficult to protect.** According to the findings, the most serious consequence of data loss and exfiltration is non-compliance with regulations. As shown in Figure 7, 58 percent of respondents say structured regulated data is the most difficult to safeguard. This is surprising because there are well-established techniques to detect this type of data exfiltration using current DLP solutions. This is followed by the protection of user-created unstructured data such as sensitive email content, text files, M&A documents, confidential press releases, etc. (53 percent of respondents), which typically lack a pattern.

**Figure 7. The types of data that are the most difficult to protect from data loss and exfiltration using current DLP solutions**
More than one response permitted



**End-user convenience is considered very important to organizations.** Respondents were asked to rate the importance of ensuring end-user convenience and avoiding disruption to the business when building and/or deploying data loss solutions in the workplace on a scale of 1=not important to 10=very important. Figure 8 presents the very important responses (7+ on the 10-point scale). As shown, 75 percent of respondents say end-user convenience is very important.

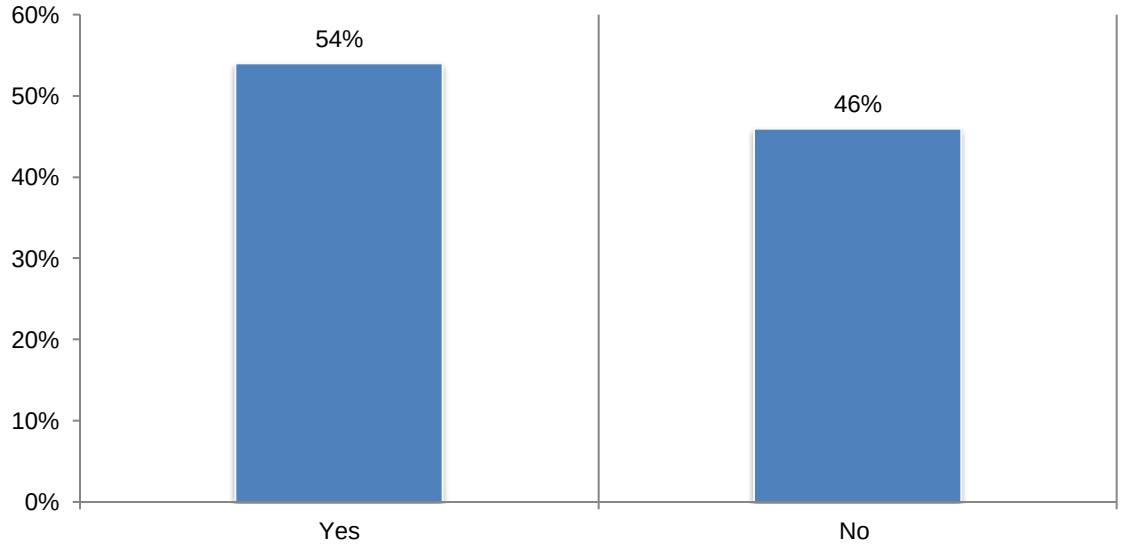
**Figure 8. The importance of end-user convenience vs. the importance of email data loss prevention**
On a scale from 1 = not important to 10 = very important (7+ responses)



**Despite the risk, many organizations do not have training and awareness programs with a focus on the sensitivity and confidentiality of data transmitted in employees' email.** Sixty-one percent of respondents say their organizations have training and awareness programs for employees and other stakeholders who have access to sensitive or confidential personal information. However, 65 percent of these respondents say training is conducted sporadically (29 percent of respondents) or only employees receiving training one time (36 percent of respondents).

As shown in Figure 9, only about half (54 percent of the 61 percent of respondents with programs) say the programs address the sensitivity and confidentiality of data in employees' email. As discussed, certain functions are more likely to put data at risk. These functions are especially in need of training that specifically addresses the risks of transmitting sensitive and confidential data in employees' email.

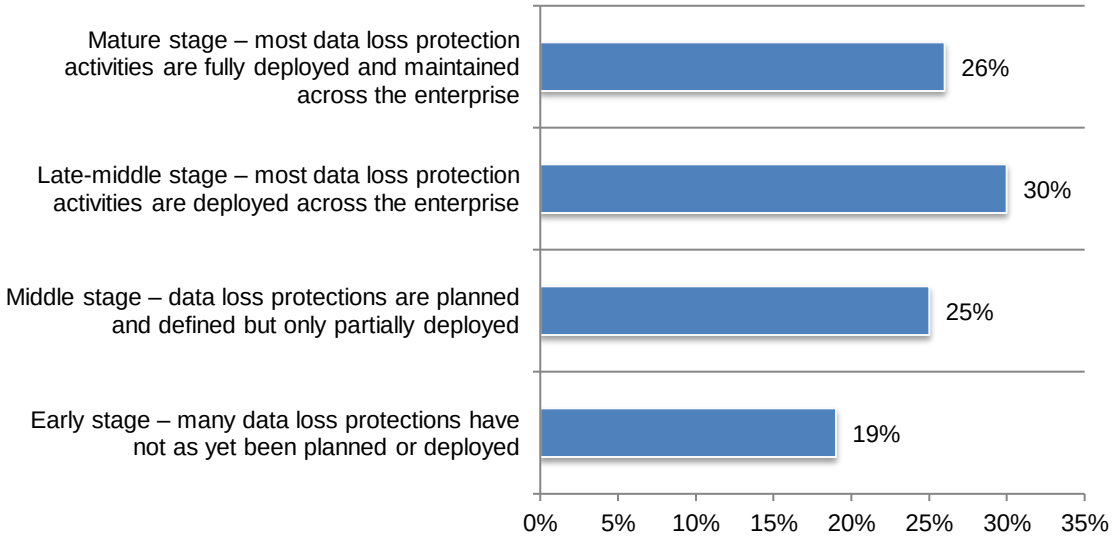
**Figure 9. Does the training and awareness program address the sensitivity and confidentiality of data in employees' email?**



## The use of technologies and their effectiveness in preventing email data loss and exfiltration

**A lack of maturity in the deployment of data loss protection activities in email is putting data at risk.** Figure 10 presents the four stages of maturity in the ability to prevent sensitive data in emails from being lost or exfiltrated. Only 26 percent of respondents say most data loss protection programs are fully deployed and maintained across the enterprise and 30 percent of respondents say most programs are deployed but not maintained.

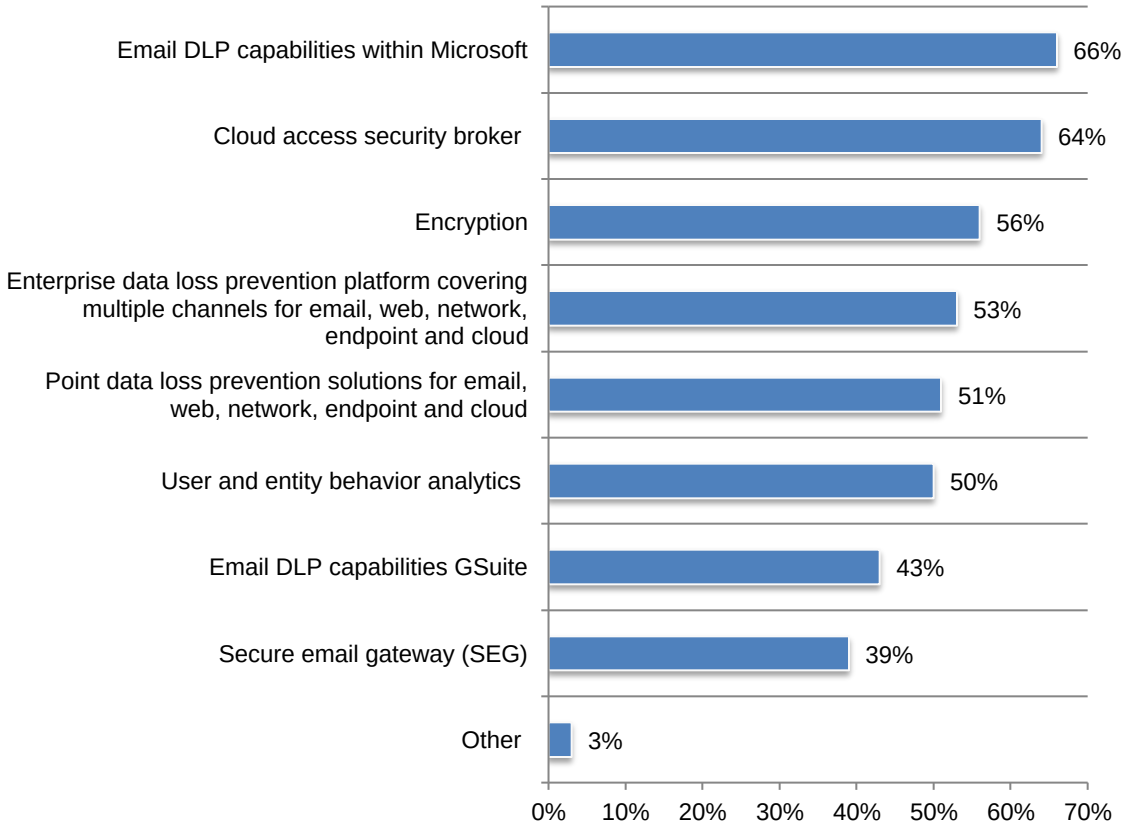
**Figure 10. What best describes the maturity of your organization's approach to protecting the loss or exfiltration of sensitive and confidential data on email?**



To prevent email-based data loss and exfiltration, 66 percent of respondents say they use email capabilities within Microsoft and 64 percent of respondents say their organizations use a Cloud Access Security Broker (CASB), as shown in Figure 11.

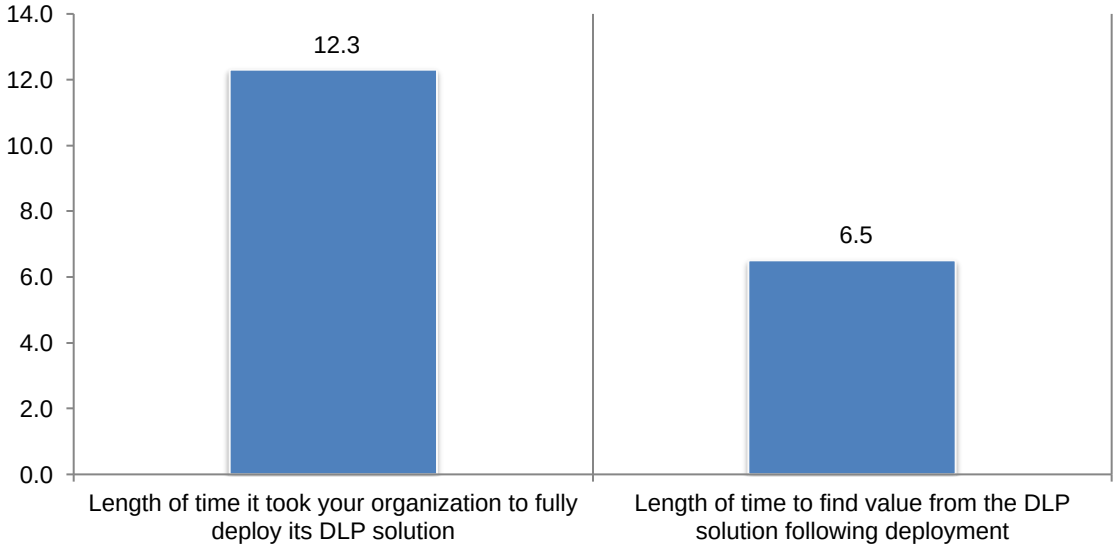
Respondents were asked to rate the effectiveness of these technologies on a scale from 1 = not effective to 10 = very effective. Only 45 percent of respondents say these technologies are very effective (7+ on the 10-point scale).

**Figure 11. What technologies are you currently using to prevent email-based data loss and exfiltration?**
More than one response permitted



**On average, it takes 18 months to deploy and find value from the DLP solution.** According to Figure 12, organizations spend an average of slightly more than a year (12.3 months) to complete deployment of a DLP solution and more than half a year (6.5 months) to realize the value of the solution with more than 25 percent of respondents reporting that it takes more than 18 months to deploy a DLP solution. The length of time to deploy and realize value can affect the ability for organizations to achieve a more mature approach to preventing email compromises by employees.

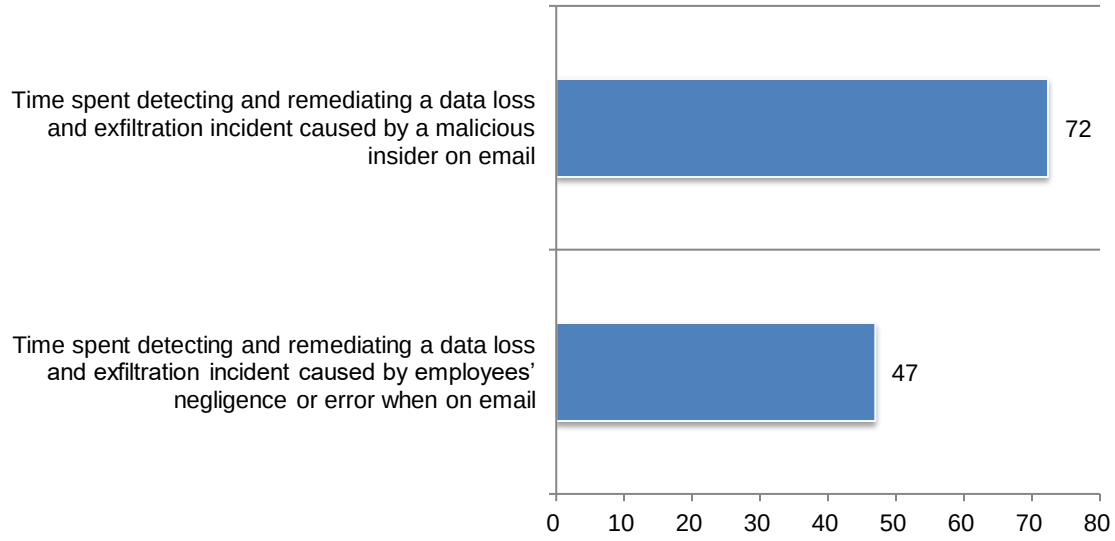
**Figure 12. Time to deploy and find value from the DLP solution**
Extrapolated value (months)



**The length of time to detect and remediate email compromises puts sensitive and confidential data at risk and places a heavy burden on security and risk management teams who are dealing with many security incidents at the same time.** According to the findings, in the past 12 months 59 percent of organizations represented in this research had data loss and exfiltration that involved an employee accidentally or by mistake sending an email to an unintended recipient. Forty percent of respondents say it was due to employee negligence.

As shown in Figure 13, it can take an average of 72 hours to detect and remediate a data loss and exfiltration incident caused by a malicious insider on email and an average of almost 48 hours to detect and remediate an incident caused by employees. This can place a heavy burden on already stretched security and risk management teams who must respond to email-related compromises.

**Figure 13. Time spent detecting and remediating a data loss and exfiltration incident caused by employees' or malicious insider on email**
Extrapolated values (hours)

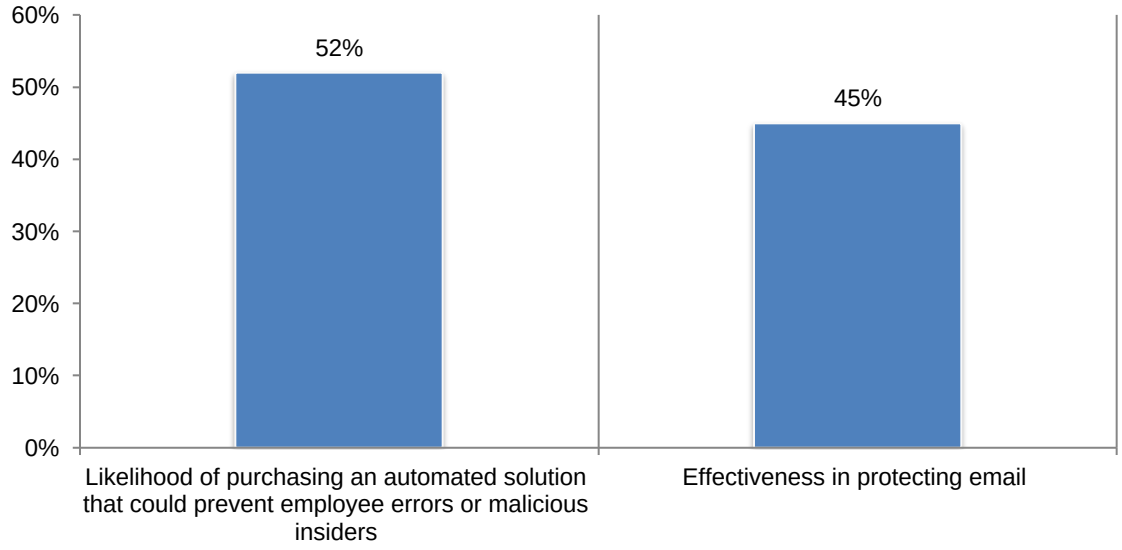


## Barriers and capabilities that improve email data loss prevention

**Technologies to prevent employee errors and malicious insider compromises are considered ineffective by many organizations.** Respondents were asked to rate the effectiveness of their existing technologies on a scale of 1 = not effective to 10 = very effective and how likely it would be to invest in an automated solution.

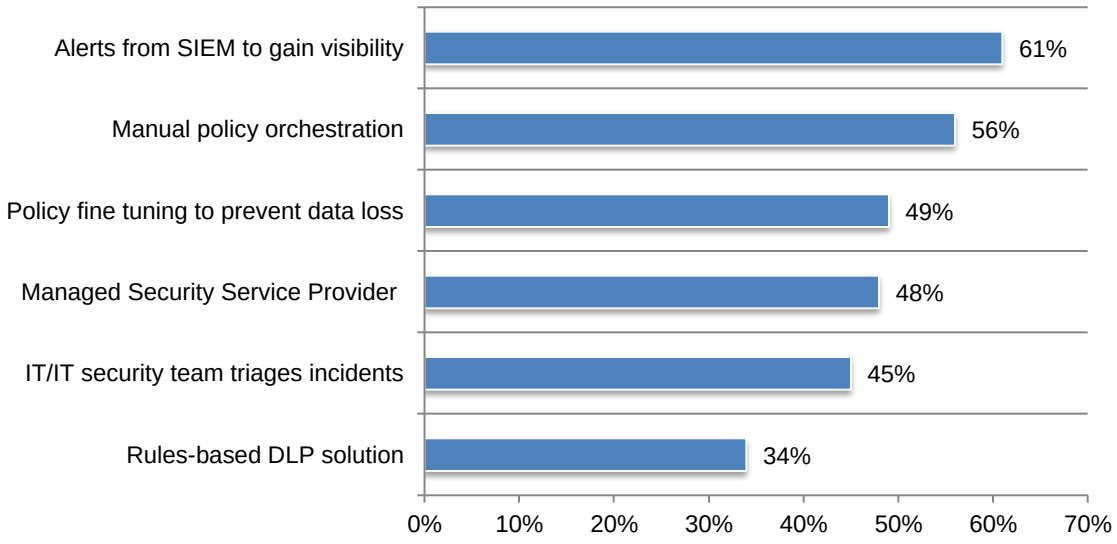
Figure 14 presents the very effective and very likely responses (7+ on the 10-point scale). As shown, only 45 percent of respondents say their technologies are very effective. However, more than half (52 percent) of respondents say their organizations are very likely to purchase an automated solution.

**Figure 14. Effectiveness of existing technologies and likelihood of purchasing an automated solution to prevent employee errors or malicious insiders**
On a scale from 1 = not effective to 10 = very effective, 1 = not likely to 10 = very likely 7+ responses presented



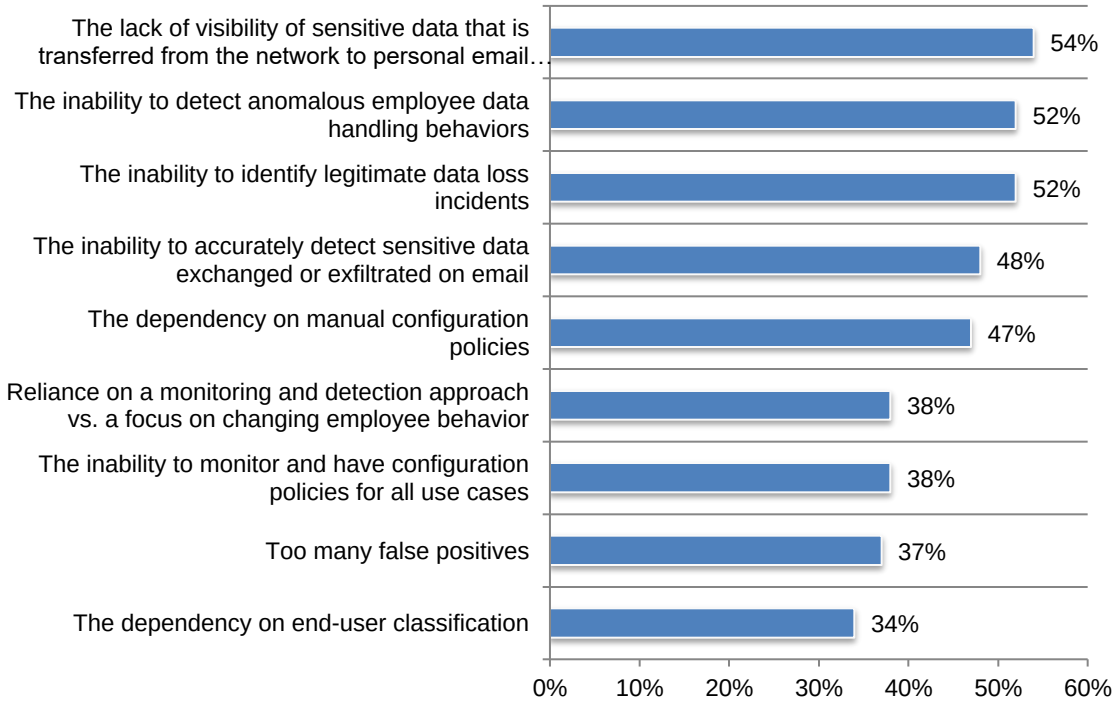
**To reduce the consequences of email data loss, organizations, organizations are using traditional security methods such as a combination of SIEM and manual policy orchestration security tools used (61 percent and 56 percent of respondents).** This is followed by policy fine tuning to prevent data loss. As discussed previously, 52 percent of respondents say their organizations are likely to purchase an automated solution.

**Figure 15. What security methods does your organization use to reduce the consequences of email data loss caused by employees?**
More than one response permitted



**Sensitive and confidential information are at risk because of the lack of visibility and the ability to detect employee negligence and errors.** According to Figure 16, 54 percent of respondents say the primary barrier to securing sensitive data is the lack of visibility of sensitive data that is transferred from the network to personal email. Fifty-two percent of respondents say it is the inability to detect anomalous employee data handling behaviors and to identify legitimate data loss incidents.

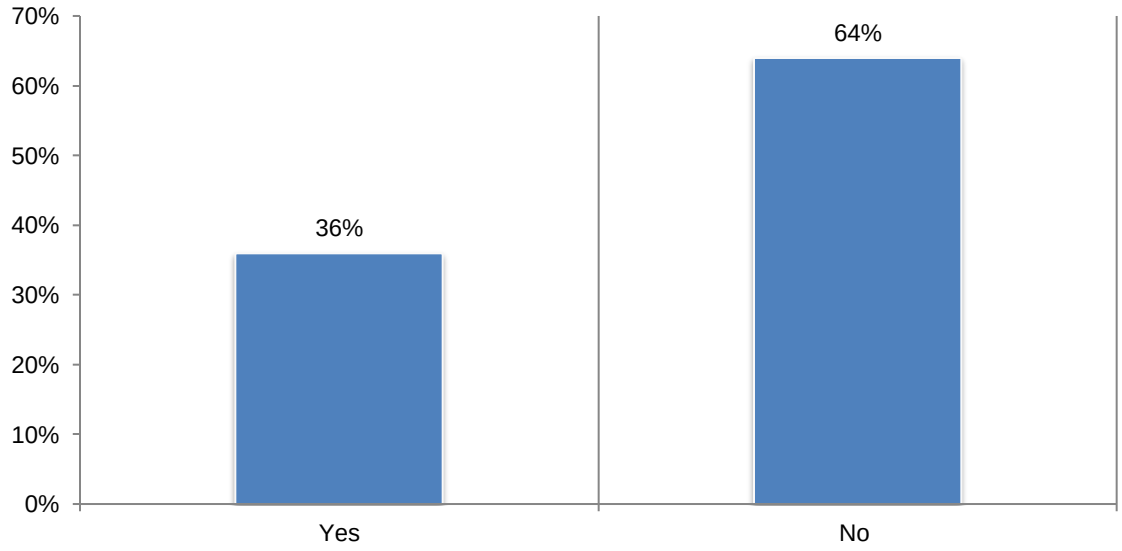
**Figure 16. What are the primary barriers to preventing email data loss and exfiltration because of employee negligence, error or intentional data exfiltration?**
Four responses permitted



**A behavioral intelligence approach is considered effective in stopping data loss and exfiltration before they happen.** In the context of this research, a behavioral intelligence approach leverages machine learning and artificial intelligence capabilities. This approach enables organizations to understand normal behavior with context from historical e-mail communication and detect behavioral anomalies to mitigate email data loss vulnerabilities. As a result, email data breaches may be stopped before they happen.

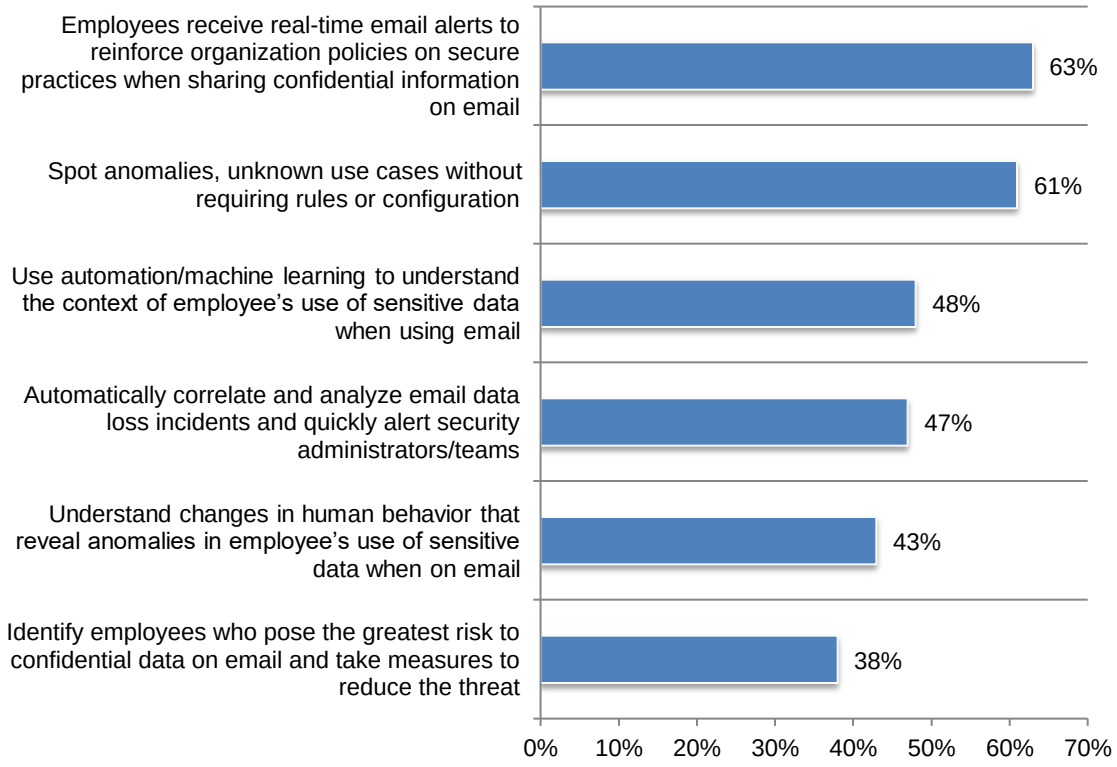
According to Figure 17, 36 percent of organizations have adopted machine learning and AI to understand human behavior. Of these respondents, 77 percent say it is effective or very effective.

**Figure 17. Does your organization use a behavioral intelligence approach to protect email from employees' negligence and error such as machine learning/artificial intelligence powered email security to understand human behavior?**



**The deployment of automation and machine learning to understand behavior and real time coaching with alerts are the top capabilities to reduce email data loss.** While the technologies listed in Figure 18 may not all be deployed in organizations represented in this research, 63 percent of respondents say providing employees with real-time alerts to reinforce organization policies on secure practices when sharing confidential information on email and spotting anomalies, unknown use cases without requiring rules or configuration (61 percent of respondents) are considered the most effective in the prevention and detection of email data loss.

**Figure 18. What capabilities will improve the prevention and detection of email data loss because of employee negligence, error or intentional data exfiltration?**
Three responses presented



## Part 3. Methodology

A sampling frame of 16,230 IT and IT security professionals who are involved in the use and management of DLP technologies that address the risks created by employees' errors or negligent email practices and familiar with their organizations' DLP solutions used to mitigate the loss or exfiltration of sensitive data were selected as participants to this survey. Table 1 shows 665 total returns. Screening and reliability checks required the removal of 51 surveys. Our final sample consisted of 614 surveys or a 3.8 percent response.

| **Table 1. Sample response** | Freq | Pct% |
|---|---|---|
| Sampling frame | 16,230 | 100.0% |
| Total returns | 665 | 4.1% |
| Rejected or screened surveys | 51 | 0.3% |
| Final sample | 614 | 3.8% |

Figure 22 reports the respondent's organizational level within participating organizations. By design, more than half (68 percent) of respondents are at or above the supervisory levels. The largest category at 15 percent of respondents is technician or staff for security.

**Figure 22. Current position within the organization**

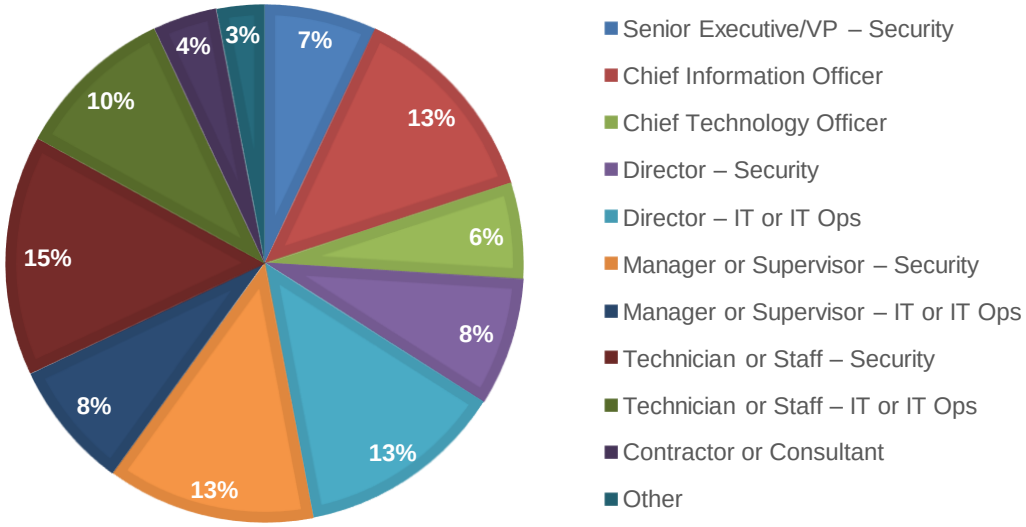
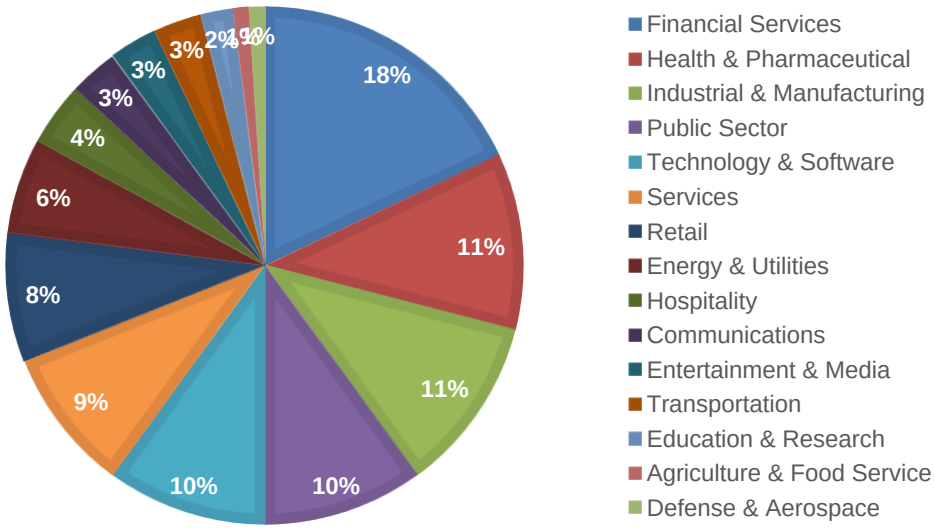


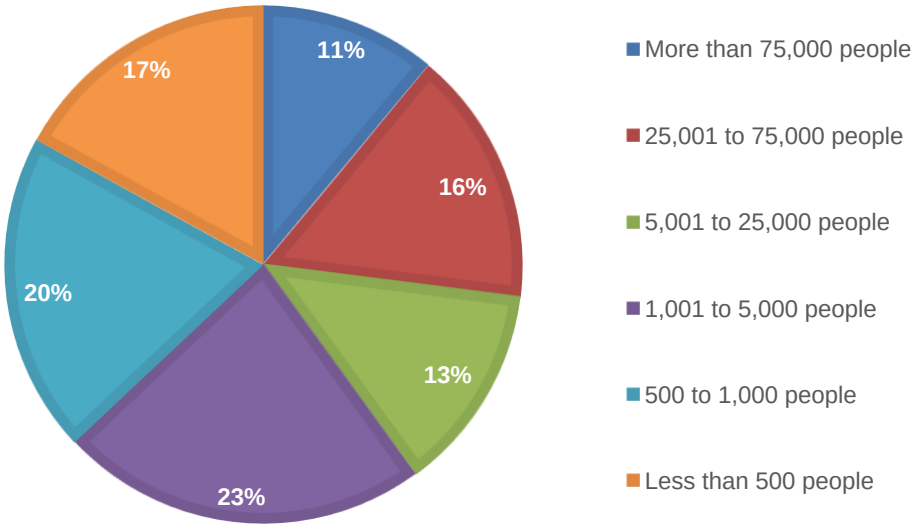
Figure 23 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceuticals (11 percent of respondents), industrial and manufacturing (11 percent of respondents), public sector (10 percent of respondents), technology and software (10 percent of respondents), and services (9 percent of respondents).

**Figure 23. Primary industry focus**




As shown in Figure 24, 63 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

**Figure 24. Global full-time headcount**



## Part 4. 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, 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 IT or IT security professionals who are familiar with their organizations DLP. We also acknowledge that the results may be biased by external events such as media coverage. Finally, 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, there is always the possibility that a subject did not provide accurate responses.

## Part 5. Appendix with the detailed audited findings

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March 2022.

| **Survey response** | Freq |
|---|---|
| Total sampling frame | 16,230 |
| Total survey returns | 665 |
| Rejected surveys | 51 |
| Final sample | 614 |
| Response rate | 3.8% |

**Part 1. Screening**

| S1. Do you have any role or involvement in the use of technologies that address the risks created by employees' errors or negligent email practices? | Pct% |
|---|---|
| Yes, significant involvement | 41% |
| Yes, some involvement | 39% |
| Yes, minimal involvement | 20% |
| No involvement (Stop) | 0% |
| Total | 100% |

| S2. How familiar are you with your organization's data loss protection (DLP) solutions used to mitigate the loss or exfiltration of sensitive data? | Pct% |
|---|---|
| Very familiar | 38% |
| Familiar | 36% |
| Somewhat familiar | 26% |
| No knowledge (Stop) | 0% |
| Total | 100% |

**Part 2. Background on email security incidents**

| Q1a. Has your organization experienced data loss or exfiltration over the past 12 months that involved an employee accidentally or by mistake when using email (e.g. data sent to an unintended recipient)? | Pct% |
|---|---|
| Yes | 59% |
| No (please skip to Q2) | 41% |
| Total | 100% |

| Q1b. If yes, in the past year, approximately how many data loss and exfiltration incidents involving employees' use of email occurred **each month**? | Pct% |
|---|---|
| 1 to 5 | 7% |
| 6 to 10 | 10% |
| 11 to 15 | 10% |
| 16 to 20 | 19% |
| 21 to 30 | 23% |
| 31 to 40 | 19% |
| 41 to 50 | 6% |
| 50+ | 6% |
| Total | 100% |
| Extrapolated value | 24.67 |

| Q1c. If yes, how would you characterize the data loss and exfiltration? Please select one top choice. | Pct% |
|---|---|
| Accidental data loss | 28% |
| Employee negligence because of not following policies | 40% |
| Insider theft | 27% |
| Uncertain | 5% |
| Total | 100% |

| Q1d. What type(s) of sensitive and confidential data were lost or stolen? Please check all that apply. | Pct% |
|---|---|
| Accounting and financial information | 31% |
| Employee information, including payroll data | 43% |
| Medical data | 19% |
| Intellectual property | 56% |
| Product information | 37% |
| Customer information | 61% |
| Consumer information | 47% |
| Information about business partners | 21% |
| Total | 315% |

| Q1e. What were the consequences? Please check all that apply | Pct% |
|---|---|
| Decreased trust with customers | 36% |
| Decline in revenues | 45% |
| Decline in reputation | 52% |
| Decreased trust with business partners | 49% |
| Decreased trust with employees | 41% |
| Regulatory non-compliance | 57% |
| Regulatory fines | 18% |
| Lawsuits | 21% |
| Other (please specify) | 4% |
| Total | 323% |

| Q2. Which departments or functions are most likely to put data at risk when using email? Please select the top three departments or functions. | Pct% |
|---|---|
| Accounting | 40% |
| Business development/sales/channel | 39% |
| Client services/relationship management | 19% |
| Engineering | 23% |
| Finance | 51% |
| Human resources | 40% |
| Legal/compliance | 54% |
| Marketing/public relations | 61% |
| Operations | 57% |
| Production/manufacturing | 58% |
| Public affairs | 25% |
| Purchasing/procurement | 17% |
| Research and development | 13% |
| Other (please specify) | 3% |
| Total | 500% |

| Q3. Please rate your organization's **urgency** in securing email data loss incidents from employee negligence and errors on a scale from 1 = not urgent to 10 = very urgent. | Pct% |
|---|---|
| 1 or 2 | 13% |
| 3 to 4 | 21% |
| 5 to 6 | 23% |
| 7 to 8 | 22% |
| 9 to 10 | 21% |
| Total | 100% |
| Extrapolated value | 5.84 |

| Q4. Please rate **the importance** of end-user convenience and avoiding disruption to the business when building and/or deploying data loss solutions in the workplace from 1 = not important to 10 = very important. | Pct% |
|---|---|
| 1 or 2 | 4% |
| 3 to 4 | 5% |
| 5 to 6 | 16% |
| 7 to 8 | 35% |
| 9 to 10 | 40% |
| Total | 100% |
| Extrapolated value | 7.54 |

| Q5. Using the following 10-point scale, please rate **the importance** of email data loss prevention relative to all other mediums of data and IT security measures deployed by your organization from 1 = not important to 10 = very important. | Pct% |
|---|---|
| 1 or 2 | 9% |
| 3 to 4 | 12% |
| 5 to 6 | 15% |
| 7 to 8 | 23% |
| 9 to 10 | 41% |
| Total | 100% |
| Extrapolated value | 7.00 |

| Q6. Which are the two most common and the riskiest medium for the loss of sensitive data by employees? Please select all that apply. | Pct% |
|---|---|
| Email | 65% |
| Instant messaging/cloud communication platforms (Slack, Microsoft Teams etc.) | 57% |
| Content collaboration platforms (SharePoint, Google Drive) | 53% |
| FTP and secure file transfers | 43% |
| Endpoint | 50% |
| Cloud services (Dropbox, Box etc.) | 62% |
| Other (please specify) | 2% |
| Total | 332% |

**Part 3. How prepared is your organization to minimize data loss through email risks? Please rate each statement using the 10-point scale from 1 = not effective to 10 = very effective**

| Q7. How effective are your current data loss prevention solutions in preventing data loss incidents caused by employees from 1 = not effective to 10 = very effective? | Pct% |
|---|---|
| 1 or 2 | 14% |
| 3 to 4 | 21% |
| 5 to 6 | 24% |
| 7 to 8 | 20% |
| 9 to 10 | 21% |
| Total | 100% |
| Extrapolated value | 5.76 |

| Q8. How effective is your organization in preventing accidental data loss caused by misdirected emails with files attached not intended for the recipient from 1 =not effective to 10 = very effective? | Pct% |
|---|---|
| 1 or 2 | 23% |
| 3 to 4 | 21% |
| 5 to 6 | 24% |
| 7 to 8 | 20% |
| 9 to 10 | 12% |
| Total | 100% |
| Extrapolated value | 5.04 |

**Please rate each statement using the 10-point scale from 1 = not concerned to 10 = very concerned**

| Q9. How concerned is your organization that its employees do not understand the sensitivity and confidentiality of data that they share through email from 1 = not concerned to 10 = very concerned? | Pct% |
|---|---|
| 1 or 2 | 10% |
| 3 to 4 | 6% |
| 5 to 6 | 11% |
| 7 to 8 | 35% |
| 9 to 10 | 38% |
| Total | 100% |
| Extrapolated value | 7.20 |

| Q10. How much of a business priority will the prevention of data loss and exfiltration via Microsoft Teams, OneDrive and Sharepoint be from 1 = not a priority to 10 = high priority? | Pct% |
|---|---|
| 1 or 2 | 6% |
| 3 to 4 | 7% |
| 5 to 6 | 13% |
| 7 to 8 | 36% |
| 9 to 10 | 38% |
| Total | 100% |
| Extrapolated value | 7.36 |

| Q11. How will your organization safeguard sensitive and confidential data when using cloud communication channels? Please select only one choice. | Pct% |
|---|---|
| Rely upon protection built into Microsoft or Google | 32% |
| Rely upon built-in features provided in each cloud communication channel (e.g. capabilities in Dropbox, Box, Slack, Workday, etc.) | 27% |
| Use a dedicated third-party solution | 36% |
| Other (please specify) | 5% |
| Total | 100% |

**Part 4. The use of technologies to prevent data loss and exfiltration through email**

| Q12. What best describes the maturity of your organization's approach to protecting the loss or exfiltration of sensitive and confidential data on email? | Pct% |
|---|---|
| **Early stage** – many data loss protections have not as yet been planned or deployed. Response to data losses and exfiltration due to an insiders' email use is negligent is reactive and ad hoc. Resources are not sufficient for staffing and administration of the program. | 19% |
| **Middle stage** – data loss protections are planned and defined but only partially deployed. Efforts are being made to establish business processes and workflows to respond to data losses and exfiltration as a result of insider negligence or malicious exfiltration when using email. | 25% |
| **Late-middle stage** – most data loss protection activities are deployed across the enterprise. The program has C-level support and adequate resources. | 30% |
| **Mature stage** – most data loss protection activities are fully deployed and maintained across the enterprise. C-level executives are regularly informed about the effectiveness of the program. Program activities are measured with KPIs. | 26% |
| Total | 100% |

| Q13. What types of data loss or exfiltration is your organization most concerned about? Please select the top three. | Pct% |
|---|---|
| Loss or theft of customer information | 56% |
| Loss or theft of employee personal data | 43% |
| Loss or theft of medical data | 17% |
| Loss or theft of consumer data | 45% |
| Loss or theft of intellectual property | 60% |
| Loss or theft of payment card data | 41% |
| Loss or theft of strategic business information such as mergers and acquisitions | 34% |
| Other (please specify) | 4% |
| Total | 300% |

| Q14a. Does your organization use human layer security to protect e-mail from employees' negligence and error (e.g. machine learning/artificial intelligence powered email security to understand human behavior)? | Pct% |
|---|---|
| Yes | 36% |
| No (please skip to Q15a) | 64% |
| Total | 100% |

| Q14b. If yes, how effective is human layer security (as defined in this research) in protecting email on a scale from 1 = not effective to 10 = very effective? | Pct% |
|---|---|
| 1 or 2 | 5% |
| 3 to 4 | 6% |
| 5 to 6 | 12% |
| 7 to 8 | 43% |
| 9 to 10 | 34% |
| Total | 100% |
| Extrapolated value | 7.40 |

| Q15a. What technologies are you currently using to prevent email-based data loss and exfiltration? Please check all that apply. | Pct% |
|---|---|
| Encryption | 56% |
| Enterprise data loss prevention platform covering multiple channels for email, web, network, endpoint and cloud | 53% |
| Point data loss prevention solutions for email, web, network, endpoint and cloud | 51% |
| Cloud access security broker (CASB) | 64% |
| Email DLP capabilities within Microsoft | 66% |
| Email DLP capabilities GSuite | 43% |
| User and entity behavior analytics (UEBA) | 50% |
| Secure email gateway (SEG) | 39% |
| Other (please specify) | 3% |
| Total | 425% |

| Q15b. If your organization uses any of these technologies, how effective are they in protecting email on a scale from 1 = not effective to 10 = very effective? | Pct% |
|---|---|
| 1 or 2 | 14% |
| 3 to 4 | 21% |
| 5 to 6 | 20% |
| 7 to 8 | 25% |
| 9 to 10 | 20% |
| Total | 100% |
| Extrapolated value | 5.82 |

| Q16. What is the likelihood of your organization purchasing an automated solution that could prevent employee errors or malicious insiders from 1 = not likely to 10 = very likely? | Pct% |
|---|---|
| 1 or 2 | 12% |
| 3 to 4 | 25% |
| 5 to 6 | 21% |
| 7 to 8 | 22% |
| 9 to 10 | 30% |
| Total | 100% |
| Extrapolated value | 6.16 |

| Q17. What types of data are the most difficult to protect from data loss and/or data exfiltration with your organization's existing DLP solutions? Please select the top two. | Pct% |
|---|---|
| User-created unstructured data (sensitive email content, text files, M&A documents, confidential press releases etc.) | 53% |
| Partially structured data such as forms and invoices | 41% |
| Structured regulated data such as credit card data, insurance, Social Security numbers, national ID numbers, employee data | 58% |
| Intellectual property including trade secrets | 43% |
| Other (please specify) | 5% |
| Total | 200% |

| Q18. Which regulations or regulatory bodies is your organization subject to? Please check all that apply. | Pct% |
|---|---|
| Health Insurance Portability and Accountability Act (HIPAA) | 46% |
| California Consumer Privacy Act (CCPA) | 55% |
| Payment Card Industry Data Security Standard (PCI DSS) | 49% |
| General Data Protection Regulation (GDPR) | 69% |
| Financial Industry Regulatory Authority (FINRA) | 63% |
| Solicitors Regulation Authority (SRA) | 27% |
| Securities and Exchange Commission (SEC) | 34% |
| Federal Information Security Management Act (FISMA) | 31% |
| Other (please specify) | 3% |
| Total | 377% |

| Q19. What security methods does your organization use to reduce the consequences of email data loss caused by employees? Please select t all that apply. | Pct% |
|---|---|
| Rules-based DLP solution | 34% |
| IT/IT security team triages incidents | 45% |
| Policy fine tuning to prevent data loss | 49% |
| Manual policy orchestration | 56% |
| Alerts from SIEM to gain visibility | 61% |
| Managed Security Service Provider (MSSP) | 48% |
| Total | 293% |

| Q20. What are the primary barriers to preventing email data loss exfiltration because of employee negligence, error or intentional data exfiltration? Please select the top four choices. | Pct% |
|---|---|
| The inability to identify legitimate data loss incidents | 52% |
| The lack of visibility of sensitive data that is transferred from the network to personal email and collaboration platforms | 54% |
| The inability to detect anomalous employee data handling behaviors | 52% |
| The inability to accurately detect sensitive data exchanged or exfiltrated on email | 48% |
| The inability to monitor and have configuration policies for all use cases | 38% |
| The dependency on end-user classification | 34% |
| The dependency on manual configuration policies | 47% |
| Reliance on a monitoring and detection approach vs. a focus on changing employee behavior | 38% |
| Too many false positives | 37% |
| Total | 400% |

| Q21. What primary capabilities will improve the prevention and detection of email data loss because of employee negligence, error or intentional data exfiltration? Please select the top three choices. | Pct% |
|---|---|
| Understand changes in human behavior that reveal anomalies in employee's use of sensitive data when on email | 43% |
| Use automation/machine learning to understand the context of employee's use of sensitive data when using email | 48% |
| Spot anomalies, unknown use cases without requiring rules or configuration | 61% |
| Employees receive real-time email alerts to reinforce organization policies on secure practices when sharing confidential information on email | 63% |
| Automatically correlate and analyze email data loss incidents and quickly alert security administrators/teams | 47% |
| Identify employees who pose the greatest risk to confidential data on email and take measures to reduce the threat | 38% |
| Total | 300% |

**Part 5. Training and awareness for the human layer**

| Q22. Does your organization have a privacy/data protection awareness and training program for employees and other stakeholders who have access to sensitive or confidential personal information? | Pct% |
|---|---|
| Yes | 61% |
| No (please skip to Q26) | 39% |
| Total | 100% |

| Q23. How often is training conducted? Please select all that apply. | Pct% |
|---|---|
| On-boarding new employees | 42% |
| Every six months | 29% |
| Annually | 31% |
| Sporadically | 29% |
| Only once | 36% |
| Unsure | 4% |
| Total | 171% |

| Q24. Does the training and awareness program address the sensitivity and confidentiality of data employees have access to in email? | Pct% |
|---|---|
| Yes | 54% |
| No (please skip to Q26) | 46% |
| Total | 100% |

| Q25. If yes, how effective is the training and awareness program in reducing email data loss and exfiltration on a scale of 1 = not effective to 10 = very effective? | Pct% |
|---|---|
| 1 or 2 | 6% |
| 3 to 4 | 15% |
| 5 to 6 | 21% |
| 7 to 8 | 38% |
| 9 to 10 | 20% |
| Total | 100% |
| Extrapolated value | 6.52 |

**Part 6. Deployment of DLP and Budget**

| Q26. How many full time IT and IT security personnel are involved in securing sensitive and confidential data in employees' email as part of DLP? | Pct% |
|---|---|
| 1 to 5 | 15% |
| 6 to 10 | 21% |
| 11 to 25 | 29% |
| More than 25 | 35% |
| Total | 100% |
| Extrapolated value | 13.0 |

| Q27. How long did it take your organization to fully deploy its DLP solution? | Pct% |
|---|---|
| Less than 5 days | 5% |
| 1 week to 3 weeks | 6% |
| 1 month to 4 months | 9% |
| 5 months to 7 months | 11% |
| 8 months to 12 months | 28% |
| 13 months to 18 months | 16% |
| 19 months to 24 months | 14% |
| More than 24 months | 11% |
| Total | 100% |
| Extrapolated value | 12.30 |

| Q28. When did your organization find value from the DLP solution following deployment? | Pct% |
|---|---|
| Less than 5 days | 12% |
| 1 week to 3 weeks | 13% |
| 1 month to 4 months | 27% |
| 5 months to 7 months | 14% |
| 8 months to 12 months | 19% |
| 13 months to 18 months | 8% |
| 19 months to 24 months | 3% |
| More than 24 months | 4% |
| Total | 100% |
| Extrapolated values (months) | 6.52 |

| Q29. On average, how much time is typically spent detecting and remediating a data loss and exfiltration incident caused by employees' negligence or error when on email? | Pct% |
|---|---|
| Less 1 hour | 2% |
| 1 to 4 hours | 5% |
| 5 to 10 hours | 8% |
| 11 to 15 hours | 9% |
| 16 to 23 hours | 21% |
| 1 day to 2 days | 32% |
| 3 days to 5 days | 13% |
| More than 1 week | 10% |
| Total | 100% |
| Extrapolated value (Days) | 46.92 |

| Q30. On average, how much time is typically spent detecting and remediating a data loss and exfiltration incident caused by a malicious insider on email? | Pct% |
|---|---|
| Less 1 hour | 0% |
| 1 to 4 hours | 3% |
| 5 to 10 hours | 5% |
| 11 to 15 hours | 11% |
| 16 to 23 hours | 10% |
| 1 day to 2 days | 27% |
| 3 days to 5 days | 21% |
| More than 1 week | 23% |
| Total | 100% |
| Extrapolated value | 72.40 |

| Q31. What range best describes your organization's annual IT security budget in 2022? | Pct% |
|---|---|
| Less than $1 million | 5% |
| $1 to $10 million | 21% |
| $11 to $25 million | 29% |
| $26 to $50 million | 33% |
| $51 to $100 million | 8% |
| $101 to $250 million | 3% |
| $251 to $500 million | 1% |
| More than $500 million | 0% |
| Total | 100% |
| Extrapolated value (US$ millions) | $ 34.0 |

| Q32. What percentage of the IT security budget is allocated to DLP solutions? | Pct% |
|---|---|
| None | 0% |
| Less than 5% | 4% |
| 5% to 10% | 8% |
| 11% to 15% | 16% |
| 16% to 20% | 15% |
| 21% to 30% | 23% |
| 31% to 50% | 21% |
| More than 50% | 13% |
| Total | 100% |
| Extrapolated value | 28% |

| Q33a. How would you describe the budget for preventing data loss and exfiltration? Please select one choice. | Pct% |
|---|---|
| More than adequate (please skip to Part 7) | 20% |
| Adequate (please skip to Part 7) | 39% |
| Inadequate | 41% |
| Total | 100% |

| Q33b. If inadequate, would any of the following factors influence your organization to increase the budget? Please select your top three concerns. | Pct% |
|---|---|
| New regulations | 55% |
| A serious hacking incident affecting your organization | 54% |
| Media coverage of a serious hacking incident affecting another organization | 39% |
| Government incentives such as tax credits | 21% |
| Concern over potential loss of revenues due to a security incident | 34% |
| Concern over potential loss of customers due to a security incident | 40% |
| Concern over relationship with business partners and other third parties | 55% |
| Other (please specify) | 4% |
| Total | 300% |

**Part 7. Role and demographics**

| D1. What best describes your current position? | Pct% |
|---|---|
| Senior Executive/VP – Security | 7% |
| Chief Information Officer | 13% |
| Chief Technology Officer | 6% |
| Director – Security | 8% |
| Director – IT or IT Ops | 13% |
| Manager or Supervisor – Security | 13% |
| Manager or Supervisor – IT or IT Ops | 8% |
| Technician or Staff – Security | 15% |
| Technician or Staff – IT or IT Ops | 10% |
| Contractor or Consultant | 4% |
| Other (please specify) | 3% |
| Total | 100% |

| D2. What best describes your organization's industry? | Pct% |
|---|---|
| Agriculture & Food Service | 1% |
| Communications | 3% |
| Defense & Aerospace | 1% |
| Education & Research | 2% |
| Energy & Utilities | 6% |
| Entertainment & Media | 3% |
| Financial Services | 18% |
| Health & Pharmaceutical | 11% |
| Hospitality | 4% |
| Industrial & Manufacturing | 11% |
| Public Sector | 10% |
| Retail | 8% |
| Services | 9% |
| Technology & Software | 10% |
| Transportation | 3% |
| Total | 100% |

| D3. What is the worldwide headcount of your organization? | Pct% |
|---|---|
| Less than 500 people | 17% |
| 500 to 1,000 people | 20% |
| 1,001 to 5,000 people | 23% |
| 5,001 to 25,000 people | 13% |
| 25,001 to 75,000 people | 16% |
| More than 75,000 people | 11% |
| Total | 100% |

**Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.**

## 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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.