nira

Q1 2022

The Access-Risk Landscape in 2022: Trends in unauthorized data and document access

Marie Prokopets

The Access-Risk Landscape in 2022: Trends in unauthorized data and document access

This review of the global Access-Risk landscape shows that unauthorized data and document access are becoming top concerns for organizations as employees handle more data through mobile applications and cloud services. Numerous studies show the number of employees accessing documents outside firewalls and accessing unauthorized data is increasing. In the past year, a majority of organizations experienced unauthorized data and document access. When this occurs, identifying and remediating the access gaps is becoming more expensive: in 2020, it was costing $645,000 on average to clean up these incidents, according to a 2020 study from the Ponemon Institute. Overwhelmingly the access issues stem from employee error or negligence rather than from the actions of malicious insiders. We argue a solution will be based on a supportive and holistic approach that educates and enlists employees in proper Access-Risk practices.

> **"Panasonic confirms cyberattack and data breach," "Robinhood's data breach involved over 7 million customers," "Leaked slides on production stoppage obliterate Peloton market cap."**

If news headlines and received notions about document- and data security were your guide, you could be forgiven for equating data breaches with increasingly rampant cybercrime and security threats. The data tell a different story.

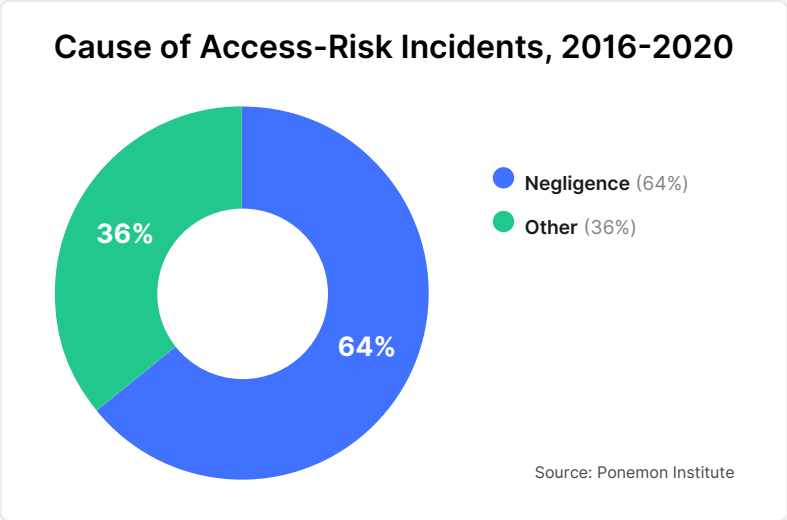
In fact, while cybercrime is a real problem, most cases of unauthorized data and document access do not originate with shadowy hackers or traitorous employees. The cause is something much more routine and ubiquitous, and so more complicated: human error.

Survey after survey has demonstrated that well-intentioned employees are the number one cause of unauthorized data and document access. The underlying reasons — negligence, mistakes, overlooked details — are a result of human nature.

To take the Peloton incident as an example: although an insider might have leaked the material to news media, the ultimate cause of the leak can be traced to a mishandling of material information. Somehow, the leaker — against which Peloton later sought legal action — was able to access, copy, and share the sensitive slides.

Also hiding within recent headlines about breaches is the magnitude of the impact. It's not just reputations that can suffer. Unauthorized access can lead to distracting and damaging incidents that distract employees, erode morale, and damage financial strength.

The Peloton incident led to a precipitous 27% one-day decline in the company's stock, at a time when it already was fighting off pessimism around its supply chain and inventory issues. In other words, unauthorized document access led to $2.5B in value being erased from the company's value, in a single day.



In this report, we will look at some of the themes resulting from the under-explored trend of Access-Risk:

1. More Access-Risk incidents exist than ever before, as a result of businesses migrating to the cloud and the proliferation of apps and services accessed there.
2. The vast majority of Access-Risk incidents are not malicious.
3. An Access-Risk program should take into account the realities of human behavior and imperfection.
4. The new work-life paradigm brought about by the Covid-19 pandemic is here to stay, which means an acceleration of the preexisting drift toward distributed workforces, cloud services, and toward multiple employee devices and endpoints.
5. Data are increasingly shared with third-parties: partners, customers, vendors, and contractors, meaning the old dichotomy of internal versus external threats is increasingly obsolete.
6. The cloud creates Access-Risk but also enables many of the solutions.

For all of the cited reasons, Access-Risk is the lens through which much of what passes for “insider threats” should be seen.

Access-Risk is a byproduct of ‘cloud-first’ workplaces

For example, the report you are now reading made its way through several cloud-based services before making its way to you. As such, this report itself is an example of the very Access-Risk issues we are discussing. At multiple points in its creation, this document was exposed to potential sharing with the wrong people, or might have found its way to the open web through the accidental creation of a public link. Of course, the sensitivity of this document is relatively low.

But the same services used to create it are also routinely used to collaborate on sensitive memos, share internal business metrics, or tabulate employees’ compensation levels.

Access-Risk is just the other side of the coin of the cloud's tremendous power to help us work together.

What is Access-Risk?

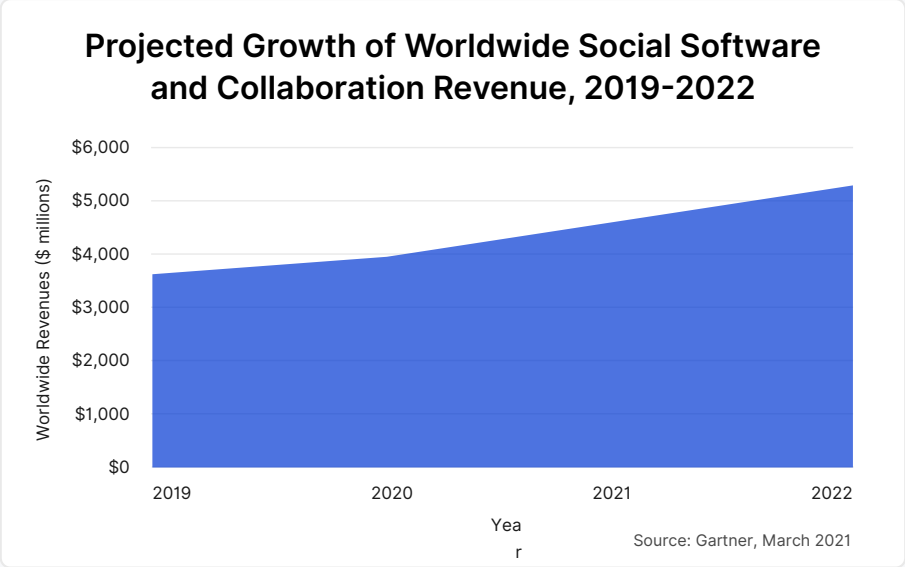
Access-Risk is an approach to data security that seeks to align an organization's data-access policies with the realities of today's workplace.

Organizations are creating more data than ever before, and this data is increasingly critical to carrying out core operational functions. At the same time, with the proliferation of collaboration tools, this data has never moved with greater ease, meaning there are an unprecedented number of exposure points for core data assets.

Responsibility for securing these data assets increasingly falls on employees who often lack the training or tools to do so effectively, or who are simply overburdened by the stresses of high growth or pressure brought on by the pandemic. As a result, the number of data breaches stemming from unauthorized access, what we call Access-Risk incidents, has risen at an alarming rate in recent years.

The vast majority of these incidents are the consequence of human error on the part of employees.

The traditional paradigm of data security, however, no longer maps onto today's flexible work arrangements. While it may generate hand-wringing among IT professionals, collaboration and a free flow of data are the norm in today's business world, and must be accommodated in a safe and secure manner.



An Access-Risk approach to data security meets these challenges by monitoring sensitive data assets and giving organizations a real-time overview into who is accessing these assets. These assets may merit strengthened, extra layers of security — passwords, encryption, pass-cards, etc. — and organizations may modify and revoke permissions to these assets as needed.

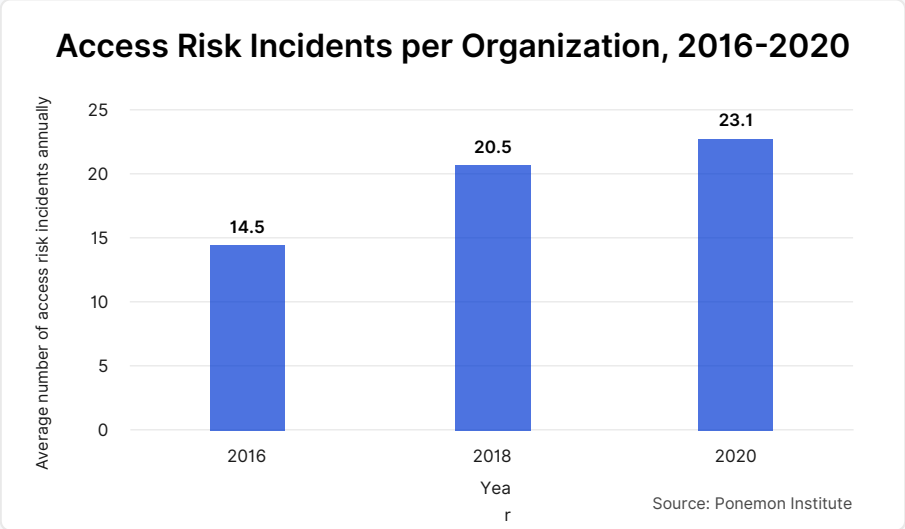
Broadly, these technologies offer proactive tools for identifying Access-Risk issues before they become costly Access-Risk incidents.

An Access-Risk approach thus seeks to work with rather than against employees, to facilitate their workflows rather than impede them. In a collaboration-based workplace, employees deserve to be treated like collaborators in managing data security. Employees are your best asset, it is often said. An Access-Risk approach to data security treats them as such.

Access-Risk: a growing and urgent problem

Access-Risk incidents are growing at a staggering rate. A survey by the Ponemon Institute found that the average number of Accident-Risk incidents per organization grew from 14.5 in 2016 to 23.1 in 2020, a stunning 59 percent increase.

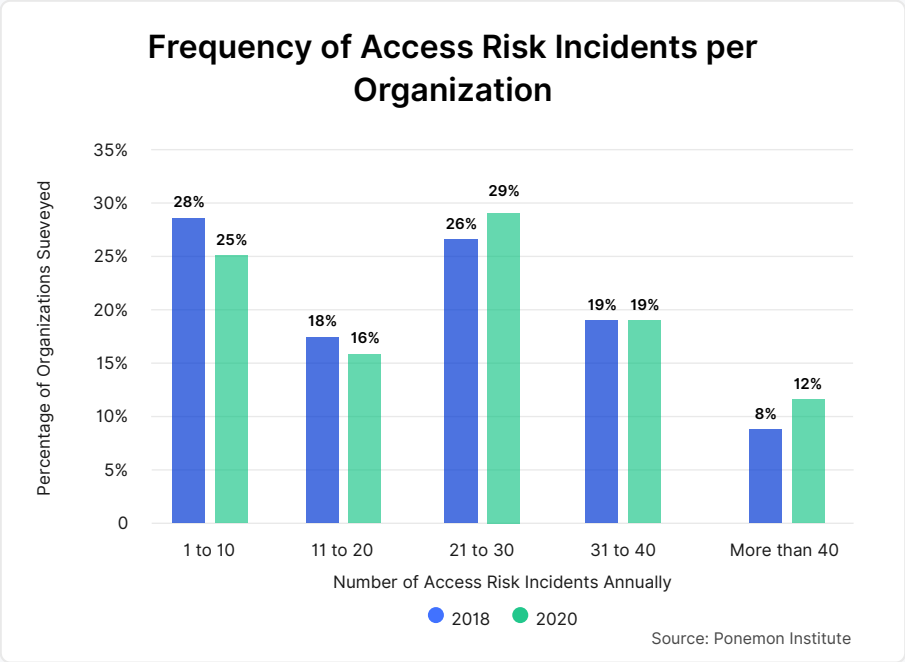
The incidents range in severity and cost, but separate research has uncovered the most damaging negative impacts. These include leaks to media that result in erosion of stock price or damage to the brand, theft of trade secrets leading to costly litigation for damages, revelation of code or data core to the operating model of the company, and loss of clients' or consumers' personal information leading to embarrassing and expensive public admissions and cleanups.



This is echoed in a separate 2020 survey of information security professionals by Cybersecurity Insiders, which found that 68 percent feel that their organization is “extremely to moderately vulnerable” to Access-Risk incidents, with the same percentage reporting that such incidents are becoming more frequent.

Also worrisome are indications the problem tends to grow worse in organizations that already face Access-Risk challenges, rather than tending to level off.

In fact, Ponemon’s study found that Access-Risk incidents were increasing most among organizations who told surveyors they already experienced 20 or more such incidents per year, accounting for some 60 percent of the organizations surveyed.



As seen above, 12 percent of these organizations experienced more than 40 Access-Risk incidents in 2020, up from 8 percent the previous year. These, as we will see shortly, come at an enormous cost to the affected organizations, and it suggests that Access-Risk issues will threaten to spiral out of control if proactive steps against the underlying causes are not taken.

Most worrisome, perhaps, is more recent data indicating a higher incidence of data breaches of all sorts after the onset of the coronavirus pandemic. Factors that commonly foster breaches were exacerbated by the sudden and haphazard shift to remote work and the new data security paradigm it has initiated.

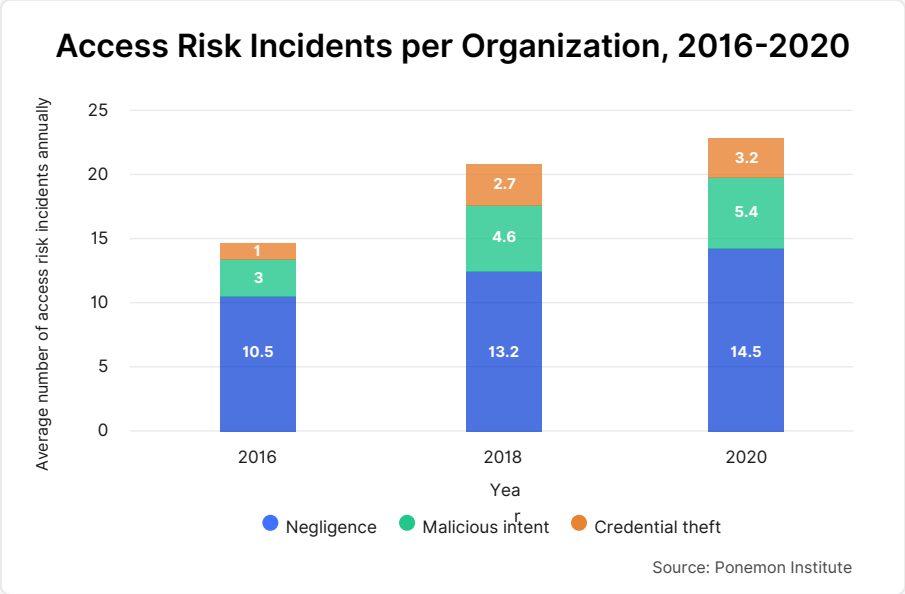
In fact, in August 2020, Verizon published a special note warning that its specialists expected breaches from multiple causes to increase as a result of pandemic-fueled dislocations.

And, it's now clear that the pandemic indeed led to a dramatic rise in the number of incidents overall. The number of cyberattack-related data compromises in the first nine months of 2021 was already 27 percent higher than the full-year total in 2020, according to the Identity Theft Resource Center in a October 2021 report.

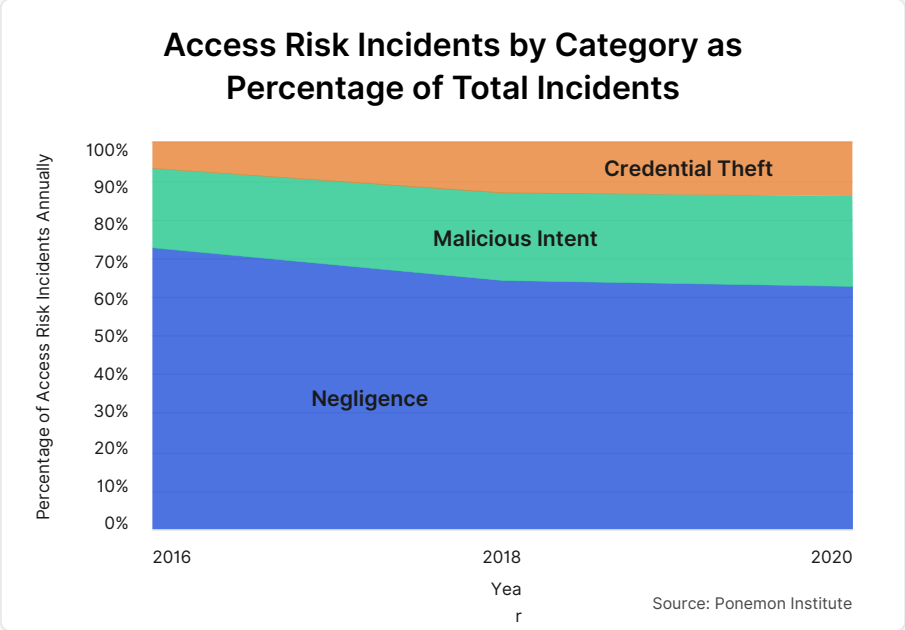
We have no reason to believe that this trend will abate. Between the ongoing uncertainty of the pandemic, the blurring of office and personal life, and the proliferation of cloud-based collaboration tools, the conditions for error—clicking the wrong link, an oversight in sharing a sensitive document—have never been riper.

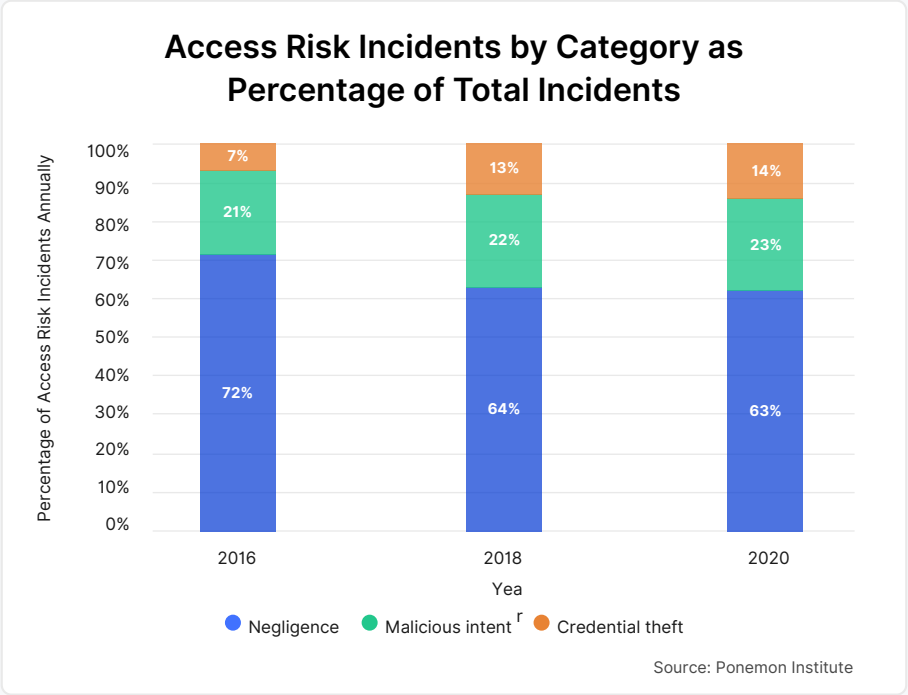
Access-Risk: to err is human

The vast majority of Access-Risk incidents are unintentional in origin. Ponemon's survey found that "employee or contractor negligence" accounted for 63 percent of Access-Risk incidents at the surveyed organizations in 2020, virtually unmoved from the year before and down slightly from 72 percent in 2016.



Credential theft has seen the largest increase, rising from 7 percent of recorded incidents in 2016 to 14 percent in 2020. However, credential theft, often originating in phishing emails or other forms of social engineering, are themselves most frequently the result of negligence. Taken together, that means that nearly 80 percent of Access-Risk incidents are the result of human error.



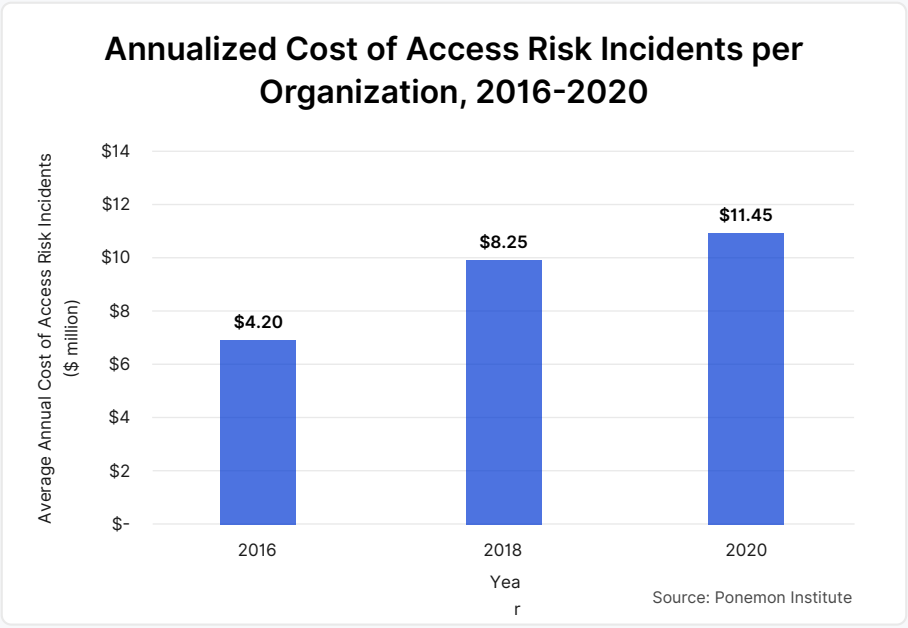


And yet that means, of course, that some incidents are not the result of innocent actions. The percentage of malicious incidents that Ponemon recorded has, however, remained steady between 21 and 23 percent between 2016 and 2020, though the number of gross incidents has been, as in all categories, on the rise. Nonetheless, it indicates that, while vigilance is always warranted, employees on the whole should not be treated like nefarious actors.

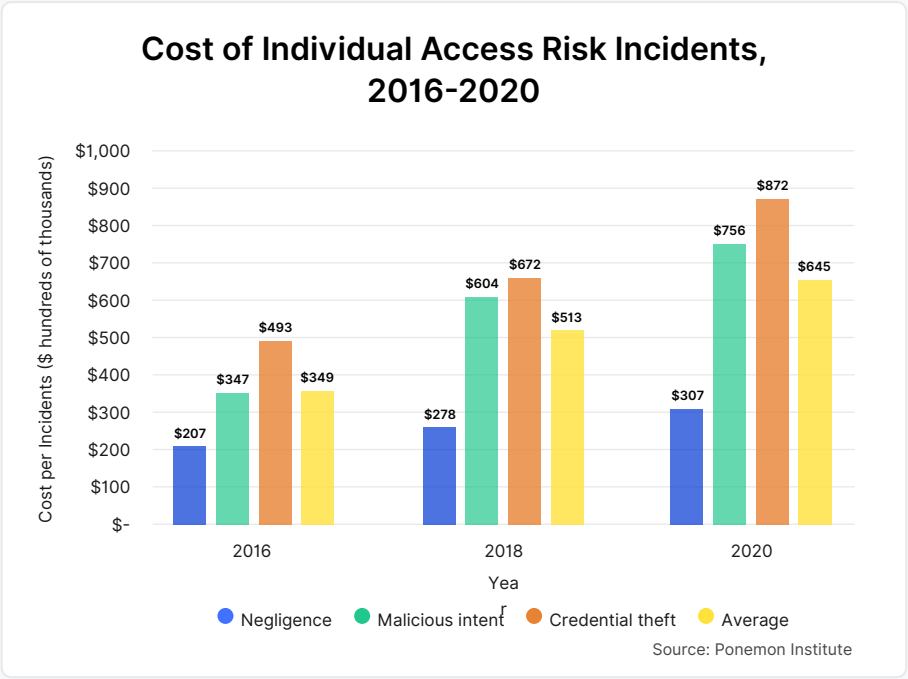
While the preponderance of unintentional incidents may be a silver lining of sorts, even benign intentions can have a ruinous effect on an organization's finances. The costs to your organization are ultimately agnostic on the origins of an Access-Risk event.

Access-Risk: a threat to your bottom line

It's not only that the number of Access-Risk incidents is increasing per year, but the cost of the incidents has been rising in tandem. The annualized cost of Access-Risk incidents to organizations surveyed by Ponemon ballooned between 2016 and 2020 from $4.2 million to $11.45 million, a staggering increase of 173 percent.



The costs associated with each individual Access-Risk incident saw significant increases in each of the aforementioned categories: an increase of 118 percent over this period for malicious incidents, 77 percent for credential theft, and a mere 48 percent increase for negligence.



On an individual basis, credential theft is the most expensive, yet least common, Access-Risk incident. Negligent Access-Risk incidents are, per incident, the cheapest of the three, yet because of their frequency they are most costly to the surveyed organizations on an annual basis.

The largest organizations surveyed, unsurprisingly, spent nearly twice as much per year resolving Access-Risk as the smallest organizations. There is little doubt, however, that the costs of an Access-Risk incident can be more detrimental to smaller organizations operating with a fraction of the budget of a multinational behemoth.

Breaking out the costs associated with Access-Risk incidents indicates that they lead to a misallocation of organizational resources. Among the least expensive costs associated with each incident, but with the highest proportion of direct costs (i.e. direct cash outlays), is the monitoring and surveillance that led to the incident's discovery. Most expensive, and with a higher proportion of indirect costs (i.e. lost labor), were incidence response, remediation, and containment.

What this suggests is that Access-Risk incidents force organizations into a reactive posture, using their valuable resources to respond to incidents that have already taken place, and that greater investment in more proactive solutions that ward off potential threats would be warranted. A 2015 Ponemon Institute study, for example, found that if employee negligence was reduced by 50 percent, an average of 31 percent of IT savings could be saved for investments in people and technology.

A final factor that merits consideration in data-breach cost is the impact of a remote-centric work culture, which became increasingly common in the wake of the pandemic. Here, the news is not encouraging, in that remote work appears to contribute to breaches going undetected for longer periods of time, and costing more overall.

For example, the 2021 IBM Cost of Data Breaches report found that breaches at organizations where more than half of employees worked remotely were $1.07 million more expensive than at companies where that was not the case (across all incidents the cost was $4.87 million per incident).

In part the greater cost was due to the longer time period it took to identify and contain breaches in companies with a tilt toward remote work. IBM found that organizations that had more than half of employees working remotely took 58 days longer to identify and contain breaches than those that did not. Across all organizations, the average time to identify and contain a data breach was 287 days.

What's at risk in Access-Risk incidents?

The cost of an Access-Risk incident is not limited to the immediate costs of its containment and may well encompass less tangible assets, such as trust, which are no less critical to an organization's success. An organization that has repeatedly experienced Access-Risk incidents may find it has fatally undermined the confidence of employees or clients or partners, as an oil spill can have a negative effect on an ecosystem long after the oil has ceased to spill.

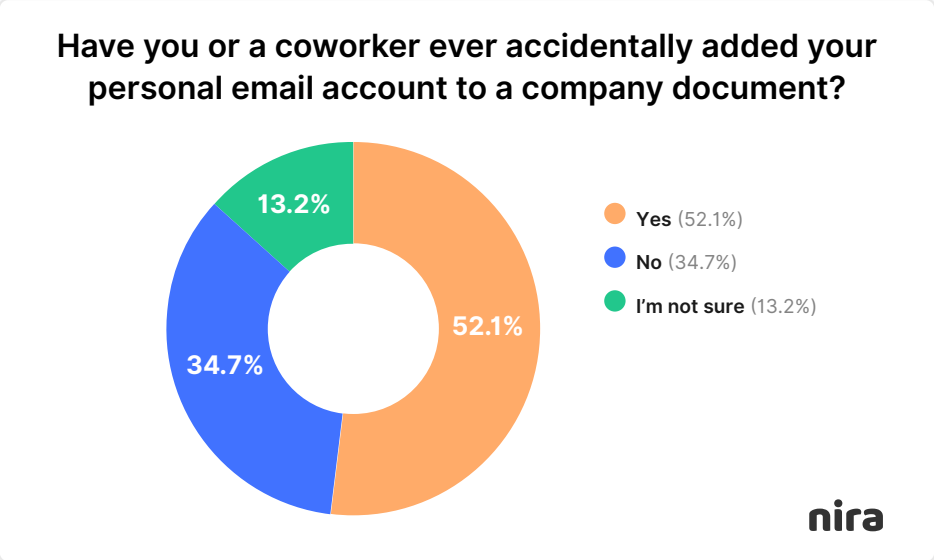
Research indicates, unfortunately, that sensitive data is as likely to be exposed in an Access-Risk incident as run-of-the-mill content. A survey of IT security professionals by Cybersecurity Insiders found that unstructured data like documents, spreadsheets, and presentations was far more difficult to secure than structured data like database records, and it is this data that is often most susceptible to the unintentional errors that precipitate the bulk of Access-Risk incidents.

According to Verizon's 2021 Data Breach Report, the number one source of data breaches involving human error is the misconfiguration or misdelivery of data assets, and the data most commonly exposed, by a large margin, is personal data. This can include, for example, names, addresses, social security numbers, etc., of employees or clients. This is information that, were it to fall into the wrong hands, would have dire consequences for those affected. And even the most benign intentions can lead to its exposure.

In 2017, for example, an employee at Boeing emailed his wife a work spreadsheet asking for help with formatting. He didn't know, however, that the spreadsheet included sensitive data on 34,000 Boeing employees, including social security numbers, in hidden columns. The data did not, thankfully, leak, but it took Boeing nearly two months to discover and contain the breach, and the incident triggered a criminal investigation. A similar data breach took place in 2018 when an employee in Alberta's Office of the Information and Privacy emailed a spreadsheet containing private information to a close contact seeking technical support.

While these seem like more clear-cut violations of data sharing policy, internal misdeliveries are no less of a problem. One study found that in an organization of 1,000 employees you can expect that there will be approximately 800 misdelivered emails per year. And the reason is simple: it's a simple error to make, as with other sources of Access-Risk incidents.

The tangle of private and professional accounts and the collaboration-tools whose use has proliferated since the pandemic began present their own template for inadvertent errors. Research from Nira, for example, found that 52 percent of respondents had accidentally added a personal account to company documents, and virtually the same percent said they had, conversely, accidentally created a document for work using a personal account.



Such documents present a range of issues for organizations. They often, for example, have public links, which facilitate document sharing, and if they are connected to private accounts IT cannot be certain who else has access to them. In the case of a document with a public link, that is anyone

with an internet connection.

It was just such a document that inadvertently exposed the plans for Britain's National Health Service's Covid-19 Health Status app when it was discovered by journalists as a public link in a different document on a Google Drive. While the damage in this case was relatively limited, thankfully, it illustrates the danger of easy Access-Risk issues inherent in the new collaboration-tools organizations have come to rely on, and a largely unresolved tension between a drive for productivity among a dispersed workforce and current data security policies and capabilities.

More worrisome, however, is what can happen to documents created and shared using these collaboration-tools after an employee leaves an organization, when their access privileges, it seems, are not always turned off. A survey by Nira found that 35 percent of respondents said they still had access to company documents in Google/Microsoft/Box/Dropbox after leaving an organization. Another 27 percent said they hadn't checked, which means that the true number could be even higher.

This is, to put it mildly, a massive risk for these companies. These documents could contain valuable intellectual property, which could end up in the hands of competitors. The same survey from Nira found that 45 percent of employees have admitted to taking documents with them before leaving an organization. Other surveys have put the number even higher.

While incidents of malicious insider abuse are relatively rare—and it is likely that many of those employees took documents without malicious intent, we will see—organizations must nonetheless remain vigilant of their occurrence, because they can have a devastating impact, sometimes threatening an organization's very existence.

Research has shown that employees are most likely to take company documents 90 days before leaving their organization, and most often in the 30 days before their departure. What this highlights is the need for organizations to adopt an Access-Risk policy that is thoroughly integrated into an employee's life cycle from start to finish, especially as it relates to offboarding.

How does Access-Risk differ from existing approaches?

Organizations have traditionally depended on data loss prevention (DLP) technologies for data security. These function by setting top-down authorization protocols by a network operator based on directives from unit managers, automatically blocking "unauthorized" parties from accessing sensitive data. Or, in addition, they may require employees to classify their own data, creating a similar, more bottom-up matrix of authorization.

In theory, this seems the most efficient, streamlined solution. In practice, these technologies no longer align with the reality of today's workplace, and may do more harm than good in protecting an organization's core data assets.

The most common complaint tied to DLP implementations is false positives, which waste the time

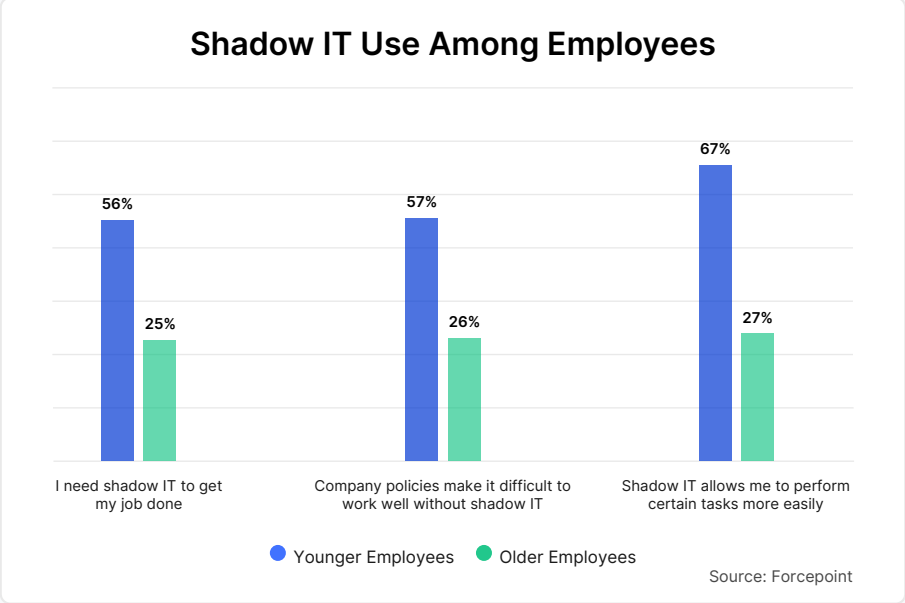
of administrators, add to the cost side of the equation in sucking up their attention, and overall make these systems highly inefficient. DLP software tends to pepper their admins with notifications, which once examined, turn out to be harmless activity. One common example: phone numbers mistakenly flagged as social security numbers.

Blind, automatic blocks can quickly become a hindrance to ordinary workflows. In a fast-paced, collaborative workplace, who is and isn't authorized to access a certain document is often a fluid situation not easily foreseen by broad, pre-established parameters.

At best, this situation can set off an unseemly number of conversations with your information security team, requiring exception carve-outs that render the original access protocols all but meaningless. At worst, it can force employees into riskier behavior in order to do their job in a timely manner. With the proliferation of messaging, file sharing, and data storage applications, both private and company-authorized, getting around a DLP's blocking system has never been easier.

We asked a security lead at one of our customers if he had ever heard of a successful DLP implementation. "No," he said flatly. "They never work."

To cite an extreme example, the managers of China's powerful "Great Firewall" have reportedly been forced to screenshot their directives for subordinates, lest they automatically be blocked for using banned words or phrases. If they can find a workaround, your employees certainly will, too. Indeed, one study found that a majority of younger employees have used "shadow IT" in performing routine job duties.

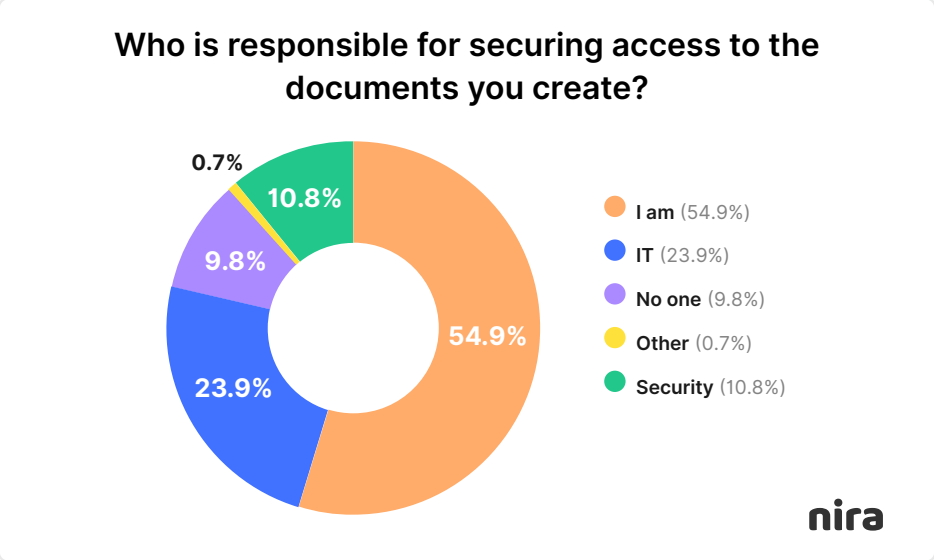


These technologies can thus, unintentionally, heighten the possibility of an Access-Risk incident. Once sensitive data has gone into an employee's private email account, it is now beyond the scope of your data security team. Their intentions were likely benign, but your team has no way of knowing who else has access to that account, whether, for example, their personal "digital hygiene"

meets your organization's professional standards.

A classification-based system runs a similar risk. In addition to an added burden on their workflow, by placing the onus of access classification on employees, one inadvertent oversight or misclassification can mean far greater access to sensitive data than intended.

According to a study by Nira, employees consider themselves responsible for securing information. But without the right tools, their efforts can go to waste, or worse yet — do more harm than good.



It is little wonder then that a Forrester survey of security leaders found that 77 percent said that these technologies were too difficult to implement and manage, and 55 percent further noted that they lacked the time or personnel needed to make them an effective solution. The number one challenge cited by respondents using these technologies was difficulty in classifying and identifying data in collaboration and file-sharing software.

The consequences of an Access-Risk incident can be devastating for an organization and, without proactive steps against their underlying causes, the likelihood of their occurrence has, unfortunately, never been higher.

A holistic approach to Access-Risk

A successful approach to Access-Risk should be interwoven into an organization's culture, and begin on day one of an employee's tenure.

The building block of any effective Access-Risk program is a clear statement on data classification and acceptable use policy, communicated during an employee's onboarding. Clear expectations should be laid out on proper device use, how employees are to secure data they handle or create, and on the overall policies and boundaries that exist.

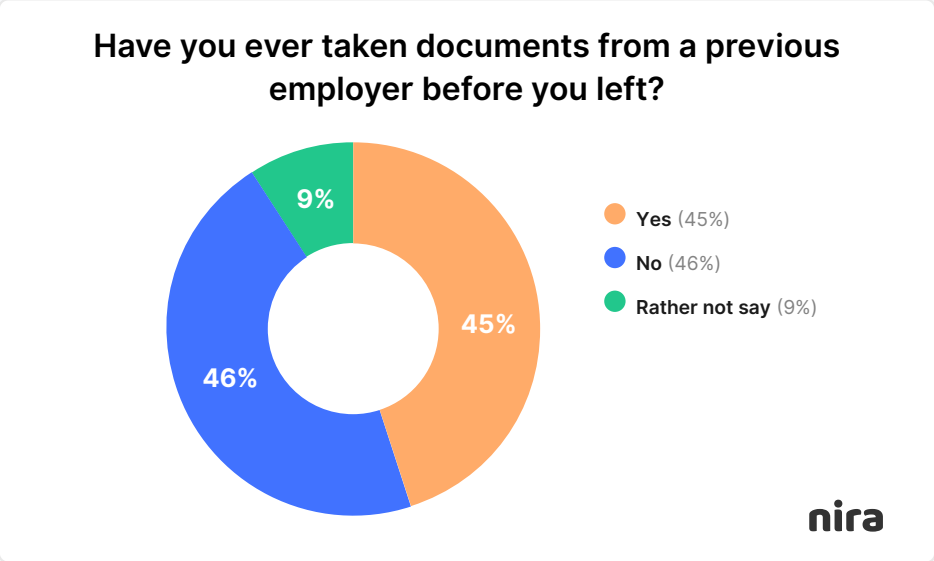
Likewise, employees should be briefed on what security software is in use, and how it works.

Otherwise, they may trip across it themselves and experience a moment of confusion or even a vague feeling of being distrusted if they're not in the know. That's counterproductive when the goal should be to enlist employees' trust, and their support in responding to instances of possible unauthorized access.

In the future, security software will flag instances of possible Access-Risk as these happen, and it should be frontline employees who have the first chance to respond, since they are best placed to do so quickly and with the proper context in mind.

Organizations should also offer advice in onboarding new employees and ensure that hires don't bring along with them documents or information from a previous employer and unwittingly attempt to infiltrate unauthorized material into your organization. If you don't want employees to exfiltrate your own data assets upon departure, you must set a company precedent in regard to bringing in outside documents as well.

Of course, it must be clearly and continually communicated in company policies that any documents an employee creates during their tenure are the property of the organization.



These data security and data use policies should be based on an organization's established workflows. If these policies contradict how employees are accustomed to working, or how they have been forced to work by the pandemic, such as the collaboration-tools we have discussed, they will not be effective, and will quickly become a hindrance and a burden.

The importance of recording data security policy and workflows illustrates how IT and security teams must come to collaborate with other departments to become integrated into an organization's DNA. IT and security, too, must take part in its organization's collaboration-culture. It can no longer afford to be an afterthought.

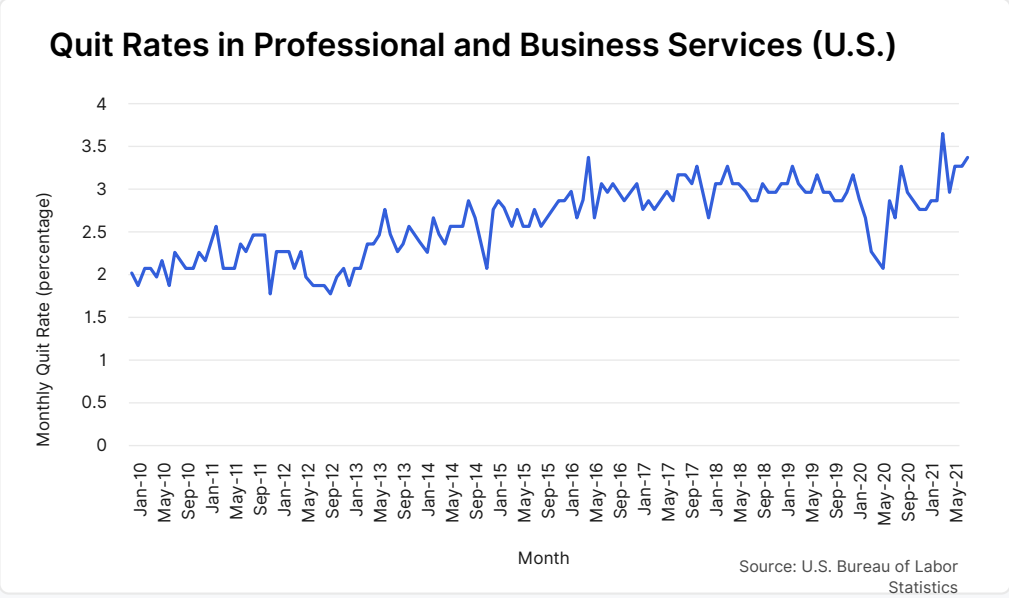
Data security policies should be continually refreshed and bolstered by regular, short trainings

throughout an employee's tenure, not limited to onboarding. These should not be an obligatory checklist, but intended to keep employees conscious of their data security practices.

Notifications can achieve a similar purpose. If IT notices an access violation—if a vendor's access to sensitive data has not been revoked, for example, or if a personal account has accidentally been added to a confidential company document—the responsible employee should be sent a notification after its resolution pointing out the problem with a friendly reminder of company policy. And this, hopefully, will offer a positive reinforcement to employee behaviors.

Creating a culture of Access-Risk awareness

Creating a culture of organizational support is crucial to a functioning Access-Risk program. Research from Carnegie Mellon's CERT institute has shown that the occurrence of employee negligence and employee malfeasance has a statistically significant negative correlation to perceived organizational support. Employees who are treated as collaborators in an organization's data security, and thus in its organizational success, will help insure the integrity of core data assets, and will minimize, further, the possibility of their exfiltration upon an employee's exit.



Offboarding, as we have noted, should be granted special attention by organizations in implementing an Access-Risk program. Not only because of the heightened possibility of core data assets being exfiltrated to competitors, but because of its frequent occurrence.

The average employee tenure today is only one and a half years. The number of voluntary departures has risen every year since 2010 according to US Bureau of Labor Statistics, and in 2019, workers quit their jobs at the fastest rate on record. This represents the proliferation of a sensitive point of possible data exposure for organizations.

As we have seen, a near-majority of employees admit to taking company documents with them upon departure (to say nothing of those who don't admit it and do it nonetheless).

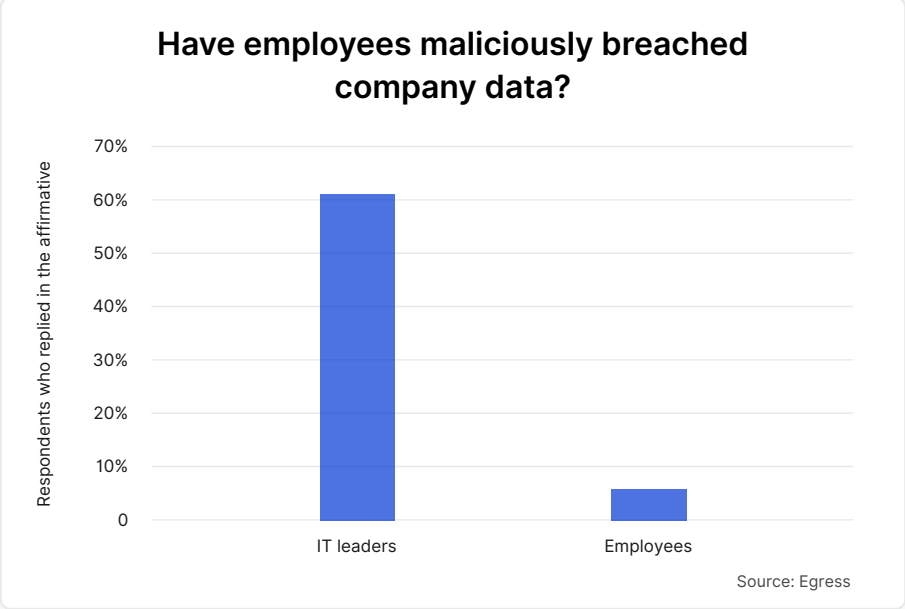
Particular vigilance, it seems, should be afforded more senior employees, who, undoubtedly, have had the greatest overview and access to core data assets. One study found that 68 percent of director-level employees take company documents with them upon exit.

The data use of departing employees should be vigorously monitored in the weeks before and after the announcement of a planned departure. Any aberrations—the use of an unauthorized USB drive, a suspiciously large file transfer, downloaded documents, emails to a private account—should be thoroughly investigated.

Upon departure, their company devices should be inspected for any irregularities that indicate data exfiltration, and their access to data assets and collaboration-tools, including access through their personal accounts, should be turned off. This last step, a bare minimum protection, is not followed through by organizations in a shocking number of cases, as we discussed above.

In an ideal situation, systems would be in place to detect aberrations, like a large takeout of email data, or abnormal sharing, ahead of any departure. After all, it is a signal that an employee might be planning to leave and take data with them.

All that said, it would be mistaken to assume that employees' taking of company documents upon departure is a clear-cut case of malicious intent. An Insider Data Breach survey from Egress 2019 found that 61 percent of the surveyed IT leaders believed that their employees have maliciously breached company data at some point. Yet the same survey found that 94 percent of American employees said they have never intentionally violated company data sharing policies.



The difference can probably be accounted for by confusion over company policy and what counts as "malicious." Many employees mistakenly believe that work they created for their employer is their personal property, whether it's a salesperson's client list or code developed by a programmer. CERT reports multiple cases in their "Insider Threat Incident Corpus" when employees took

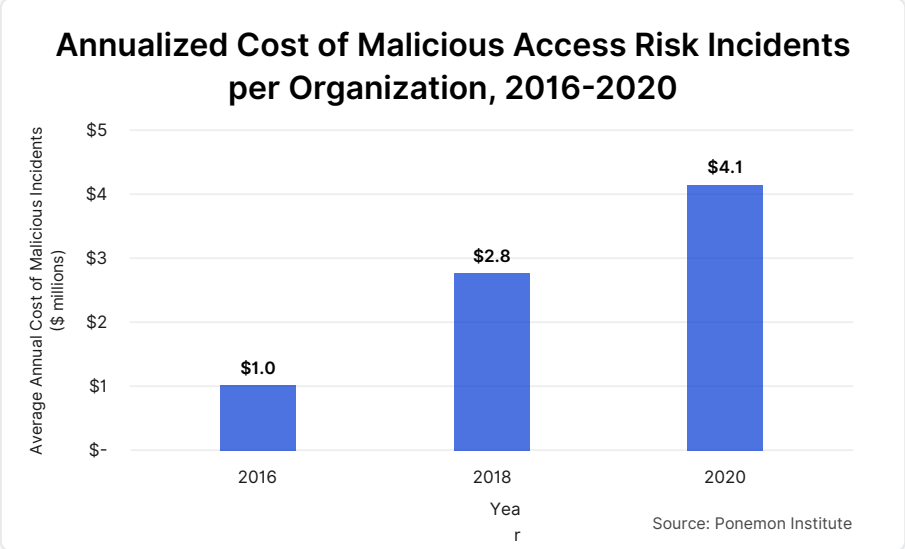
company IP with them to a new job and were surprised to find themselves accused of a crime. This underlines the importance of clearly and continually communicating that all work created by an employee during their tenure is property of the organization. And that even includes work accidentally created on their personal email accounts.

Prudence is always warranted. A shade of suspicion cast on all employees as potential "malicious insiders" is counterproductive. Such an attitude and approach to Access-Risk may have the opposite of the intended effect, actually increasing the potential for Access-Risk incidents.

Whether employees taking company data with them upon departure is always malicious in intent is open to question. There is no doubt, however, that malicious incidents can and do happen, and are worthy of an organization's vigilance.

What about those malicious insiders?

While the vast majority of Access-Risk incidents are the result of benign human error, there remains a stubborn 20 percent or so of incidents, as we have seen, that originate in malicious intent. These take up a disproportionate amount of attention in discussion of Access-Risk—unfairly, in our view—likely because the brazen theft of company secrets is more dramatic than accidentally sending an email to the wrong person. Nonetheless, a few cases in recent years demonstrate the dangers involved and why they need to be taken seriously.



The fate of Jawbone offers a cautionary tale. Once valued at $1.5 billion, Jawbone filed suit against Fitbit in 2015, accusing its competitor of luring away six of its employees along with the company's trade secrets, including 300,000 company documents.

Federal prosecutors got involved, bringing criminal trade-secret charges against the six employees in 2016, only to back away and drop them in 2020. Attorneys for the employees said there was "no case," and pointed out Jawbone had had the opportunity to examine the devices of at least one employee.

Nonetheless, the incident doubtlessly proved a distraction to all the parties involved, spotlighting why processes and policies around document access require more attention and careful enforcement.

Today, Jawbone is no longer in business despite raising nearly $1B, and Fitbit was acquired by Google for $2.1 billion.

The case of Anthony Levandowski has a happier end for the affected organization, but not for the accused individual. Levandowski co-founded Google's self-driving car project, which is now known as Waymo. He left the company in 2016 to found a startup focused on self-driving semi trucks, which was quickly acquired by Uber. In 2017, Waymo filed suit against Uber, alleging that Levandowski had downloaded 9.7 GB of confidential files and trade secrets before resigning.

The suit was reportedly initiated when one of Waymo's suppliers accidentally added a Waymo engineer on an email—misdelivery!—that revealed Uber's technology to be virtually identical to what Levandowski had developed at Waymo. Google ultimately prevailed in court, won a large settlement, while Lewandoski was ultimately sentenced to fines and prison time for trade-secret theft.

Uber shut down their self-driving truck division in 2018. And, Lewandoski — who won support from Founders Fund, a venture capital firm, and other Silicon Valley investors, executives and entrepreneurs — received a full pardon from former President Donald Trump in early 2020.

One final example occurred at McAfee, one of the leading providers of security software. A 2019 lawsuit filed by the company alleged that three sales executives took confidential documents with them to a rival, Tanium. According to the complaint, one emailed them to herself and another downloaded them to an USB stick on his last day in the office. According to McAfee, the documents held detailed information about hundreds of actual and potential McAfee sales, as well as the company's sales playbook.

A civil court denied an injunction sought by the company, however, saying McAfee had not convinced the court of the merits of its trade secrets case, and two of the defendants remained employees at Tanium as of mid-November 2021 according to LinkedIn.

But again the case served to spotlight how fraught and expensive cases of alleged unauthorized access can get.

Accidents far more common than intentional data exposure

These cases and others like them understandably attract the interest of the business press and are the stuff of executives' nightmares. But numerous data sets indicate that malicious incidents are not so prominent as the attention they are commonly afforded. Beyond the Ponemon Institute's survey that we cited earlier, Verizon's 2021 Data Breach Report found that privilege misuse, which largely encompasses malicious incidents of insider abuse, was dwarfed as a source of data

breaches by the accidental misconfiguration or misdelivery of data assets.

The key point is that a thorough Access-Risk program reduces the likelihood of all Access-Risk incidents. By thoroughly monitoring the flow of data, especially as it relates to the period before and during the offboarding process, when research indicates the majority of malicious data theft occurs, organizations can mitigate the risk of devastating incidents such as these, and no less devastating incidents originating in human error.

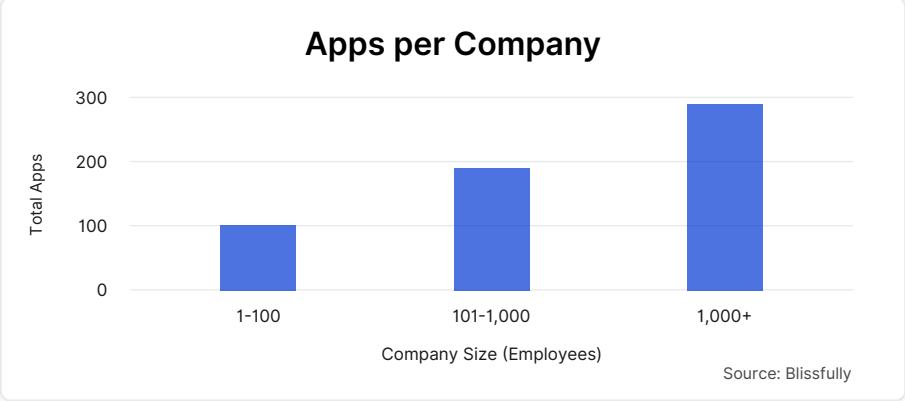
The overzealous pursuit of malicious insiders in-the-making and ominous discussion of "insider threats" (even the name has a sinister ring) is not, we believe, a helpful lens in implementing a successful Access-Risk program. The prerogative is protecting your organization's core data assets from unauthorized access, no matter its origin, and creating a positive culture around that goal.

An overemphasis on unitary "insider threats," and a rigid dichotomy between internal and external threats miscomprehends what is at stake with Access-Risk, and the possible connections between data breaches emanating from within and without. Personnel data accidentally exposed by human error, for example, could be used, in the form of credential theft, as the basis for an external attack by a criminal organization.

It is difficult to clearly delineate what constitutes "internal" and "external" when, for starters, internal is no longer defined by an office, and when the reality of today's business world is that access to sensitive data is not restricted to your own employees.

Do you know which third parties are accessing your data?

You're only as strong as your weakest link, goes a common saying. In the webbed nature of today's business ecosystem, the wisdom of this statement has never been more applicable to data security. The recent past has shown that third-party partners can often be the greatest vulnerability to a company's data assets.

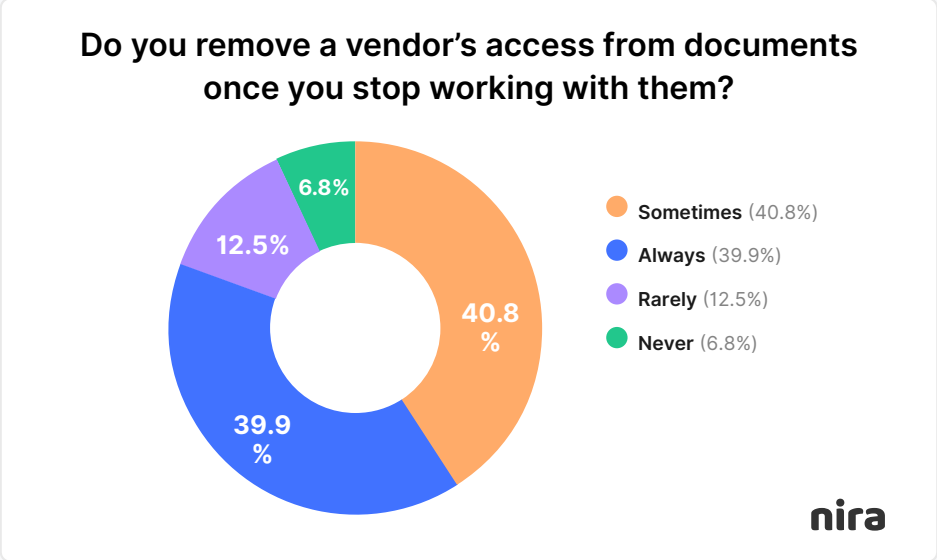


From a software perspective, the vertically integrated organization is a thing of the past. Today, companies with 101 to 1,000 employees are using an average of 185 SaaS apps, while companies with over 1,000 employees balloon to an average of 288 apps in use across all their business

operations and departments, according to Bilssfully's 2020 SaaS Trends Report. And many of these applications likely store sensitive data assets, such as source code, valuable customer information, or financial data. Or, conversely, third-party partners have access to organizations' own secure data assets.

A survey of more than 1,000 IT security professionals by One Identity found that 94 percent of their organizations granted network access to third-party users, with 72 percent of them granting privileged or superuser status. Unfortunately, however, organizations often have limited visibility into who is accessing their data. The survey of IT security professionals found that 61 percent were uncertain if third-party users—contractors, suppliers, or partners—had accessed or attempted to access unauthorized data.

It's not only that organizations do not know if third-party users are accessing unauthorized data, but their access to data persists long after it should have been turned off. Nira has found that 60 percent of organizations only sometimes, rarely, or never revoke vendor access to shared information after they are no longer working with them. Offboarding data access to outside partners should be no less important than offboarding a departing employee's access to data. They both present a vulnerability to core data assets.



The risks of this situation should be clear. A number of the most high-profile data breaches in recent years originated with vulnerabilities in third-party partners. The Target breach that affected 70 million people began when external attackers compromised an HVAC contractor with a data connection to the retailer. Delta and Sears were both subject to data breaches after a vulnerability in a customer-service chatbot was exploited. Misuse of employee credentials at a third-party application used by Marriot for guest services resulted in the information of 5.2 million guests being leaked.

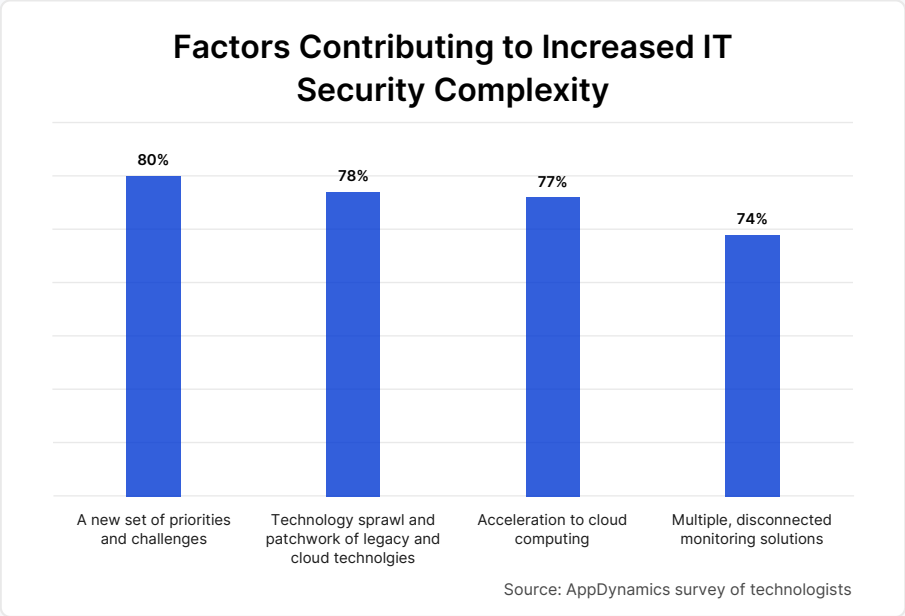
This is what we mean when we say the distinction between internal and external threats has become blurred. No business can afford to go it alone anymore, and this is why careful monitoring

of which third-party partners have access to your data assets, and which data assets, is imperative for implementing a successful data security program today.

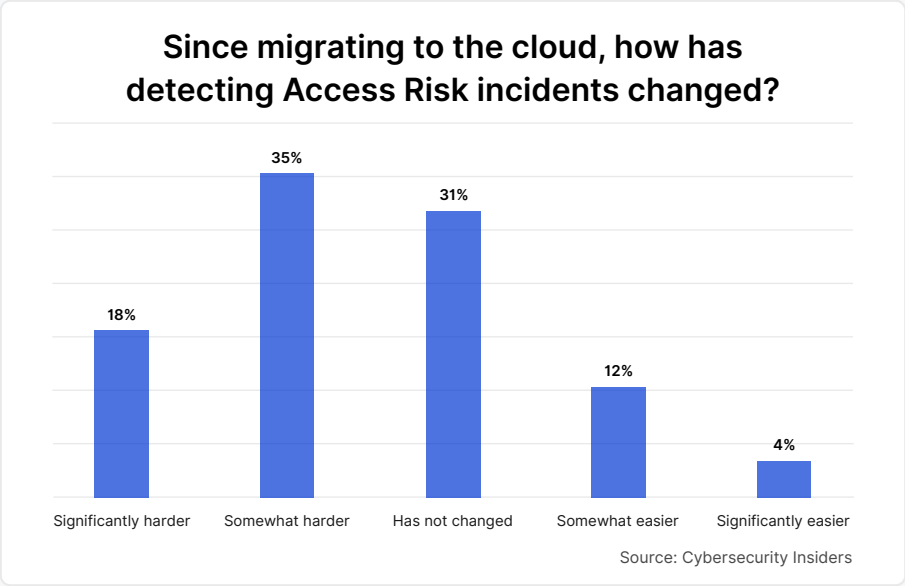
This fragmentation in the business landscape, however, is mirrored by a similar, burgeoning fragmentation in organizations' own workforces.

The impact of cloud: Low visibility on cloudy days

Remote working, whether organizations like it or not, is here to stay. By the end of summer 2020 as many as 75 percent of American office workers were working remotely, and Forrester predicts that we will see a 300 percent rise in remote working from pre-pandemic levels once work patterns settle down. Research from Pew corroborates that 54 percent of American workers wanted to continue working all or mostly from home once the pandemic has ended. And this means the new data security paradigm initiated by the pandemic is here to stay, too.



This presents a range of thorny issues for IT teams. A recent report by AppDynamics found that 83 percent of IT workers said their job has become more complex since the start of the pandemic. The chief factors complicating their work are the unwieldy combination of cloud and legacy technologies, the increased adoption of cloud computing solutions necessitated by the shift to remote work, and a tangle of disjointed monitoring solutions.



IT professionals have long been aware of the risks associated with cloud computing. A Ponemon Institute survey from 2014 found that a data breach was three times as likely to occur at a company using the cloud.

Those risks have hardly receded. According to Cybersecurity Insiders' 2020 survey of IT security professionals, 53 percent say that detecting Access-Risk incidents has become more difficult since migrating to the cloud, with only 30 percent responding that they have the capability to detect anomalous behavior in the cloud applications and infrastructure.

And yet the cloud, like the remote workforce that has accelerated its adoption, is here to stay, and organizations will have to learn to accommodate—and thoroughly monitor—its use. Much of the problem stems from the collaboration-tools we have already discussed. According to the previously cited Forrester survey, security leaders say the top challenge with current data security solutions is classifying and identifying data in collaboration and file-sharing software. With the explosion of collaboration tools, there are more points of exposure for sensitive data than ever before.

There are a number of unresolved tensions in this situation. Most Access-Risk incidents stemming from these technologies are, as we have seen, unintentional, the result of oversight in a high-stress situation using new tools. Employees, however, are increasingly expected to secure access to the documents they create. Nira found that 55 percent of employees believe they are responsible for doing so, and yet they often don't have an effective tool to help them do so.

The rise of IT outside of IT

Non-IT employees, in other words, are increasingly carrying out IT functions without proper IT tools. If employees are not integrated into a holistic culture of data security at their organization, as we discussed above, with relevant training and tools at hand, this situation will likely deteriorate. Gartner, for example, projects that 99 percent of cloud security failures through 2025 will be the customer's fault.

Other issues presented by this new paradigm are inherent in the sudden shift to a widely distributed workforce. At home, workers are using a mix of private and company-authorized devices, switching, hopefully, between a VPN and their own private network connection. This raises several issues for protecting data assets from unauthorized assets.

Besides a persistent unknowability about employees' personal "digital hygiene" and its potential to bleed back into their professional life in a setting where the two are intertwined, there is a perennial issue in sharing their work-issued devices with other members of their household. A 2018 SentinelOne report found that 55 percent of employees—pre-pandemic!—allowed friends or family members to use their work devices at home.

The potential for unauthorized access is obvious. While it is unlikely that their kids or spouses will be hacking into organizational IP, clicking on a bad link or falling for a phishing email while using the device remains a distinct possibility. And right now, it is difficult to effectively monitor that activity. According to Cybersecurity Insiders 2019 Insider Threat Report, only 27 percent of the surveyed organizations reported that they had a comprehensive monitoring of activities on- and off-network.

A related problem is emerging with the growing use of contractors and freelancers in startups, working (remotely) side-by-side with full-time staff, a phenomenon that some call "the decentralized startup." Though they may fulfill similar job functions, it is not possible, naturally, to fully integrate them into an organizational culture as you would a full-time employee.

The use of contractors presents Access-Risk issues reflected in those faced with third-party partners (both inside and out) and a remote workforce (often beyond traditional monitoring solutions). And so, an effective Access-Risk program should treat them as a combination of such, carefully monitoring their access to data assets, ensuring it does not trespass what is proscribed by their job function, and revoking access once they are no longer engaged by the company.

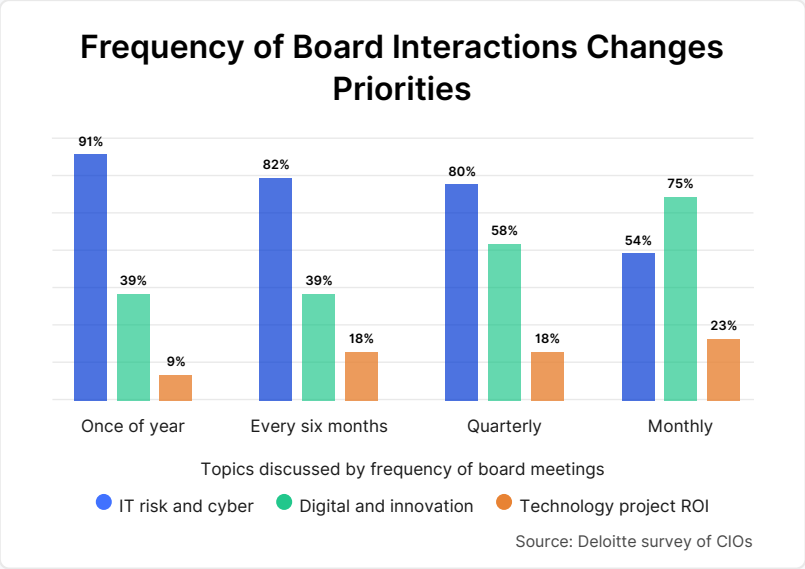
There is no doubt that these organic changes in business culture, whose germ preceded the pandemic but whose adoption was greatly accelerated by it, have made it more difficult for organizations to secure their core data assets. And yet, in addition to the challenges, there is also an opportunity for data security to finally get its due as a core business concern.

Where does Access-Risk go from here?

There is a precipitous transformation afoot in the perception of data security's importance to company success. This is especially true now that IT is no longer considered an afterthought in the organizational landscape.

A 2018 survey by Deloitte found that only 29 percent of business leaders agreed that the "technology organization and its leaders should be deeply involved in developing strategy." Two years later a different Deloitte survey found that CEOs "see technology leaders as their primary business partner, more than all other C-Suite roles combined." An Adobe/Fortune survey of CIOs found 75 percent agreeing that "their role has expanded, their responsibilities have increased, and

they have greater influence on leadership decisions within their organization," since the pandemic began.



We expect that as IT and data security becomes ingrained in organizational cultures, new tools and training will essentially make all employees, in some sense, IT-adjacent. Conversely, IT workers will necessarily become adjacent to other departments and fluent in their workflows. To achieve and solidify this change, providers of data-security solutions will need to offer tools that meet the challenges of a radically altered risk landscape.

First and foremost, this means providing proactive insight into Access-Risk issues before they become Access-Risk incidents. We expect that in the coming years this will be augmented by a growing integration of AI and machine learning capabilities into data-security solutions, providing automated, real-time reporting on potential Access-Risk issues.

These enhancements, however, will need to demonstrate their value to organizations, including, for example, their ability to operate in a complex regulatory environment. Organizations will need to feel certain they have control over software, that they understand the basis of its decisions, and that explanations and context are reported back to human administrators so that compliance becomes woven into the culture rather than only an action triggered by an isolated algorithm.

Moreover, Access-Risk technology should avoid repeating the flaws of legacy solutions, becoming a burden and a nuisance to employees' regular workflows.

We recommended earlier that employers — in companies of all sizes — openly communicate to employees about Access-Risk questions and explain why every employee has a stake in following best practices. But this does not mean that a quotient of "transparency" then serves as an excuse for using top-down technology to police a workforce. Any heavy-handed top-down intervention will only tend to undermine a culture around Access-Risk and data security, and thus would ultimately be counterproductive. Instead, the dialogue needs to shed light on security software as a helpful

tool, which can detect and point out vulnerabilities, giving companies support to sort out the implications thoughtfully. In the case of Access-Risk, document- and data-protection measures are not one-size-fits-all. The policies can and should vary widely according to industry vertical or other firmographics like company size, geography, and employee characteristics.

So by extension it will require internal expertise —from departments like compliance and legal — and the help of employees and managers who best understand the context to strike the right balance. A security policy should be perfected over years, not thrown together in the wake of a damaging incident that may lead to damaging overcompensation. Draconian policies can put a chill on collaboration, speed of decision-making, and even employee morale.

Technology alone, we believe, will never completely solve the problem of Access-Risk. A technological solution to Access-Risk will only be as effective, ultimately, as the organizational culture that utilizes it.

About Nira

Nira is a real-time access control system that is purpose-built to provide complete visibility into each and every document, employee, and external party that has access to company documents.

Time-consuming issues such as incomplete employee offboarding, hidden vendor access, and investigating incidents are effortlessly resolved with Nira.

Setup takes two minutes and then within 48-hours Nira will give you complete visibility into the state of your entire Google Drive.

Access control tasks that used to take hours, now take just a few minutes.

Get a Demo