Microsoft Security

Building a Holistic Insider Risk Management Program:

5 elements that help companies have stronger data protection and security while protecting user trust

Why companies should think about insider risk as part of their data protection strategy with a holistic approach that includes the right people, processes, and training, in addition to the appropriate tools

Report Foreword by Bret Arsenault, Chief Information Security Officer at Microsoft

The risk landscape for organizations has changed significantly in the past few years, as the digital landscape continues to grow. The amount of data captured, copied, and consumed is expected to grow to more than 180 zettabytes through 2025[1]. Traditional ways of identifying and mitigating risks simply don't work. Historically, organizations have focused on external threats; however, risks from within the organization can be just as prevalent and harmful. These internal risks include unprotected and ungoverned data, accidental or intentional data over-sharing, as well as the risks for failing to meet ever-changing regulations. Not to mention, with more than 300 million people working remotely, data is being created, accessed, shared, and stored outside of the traditional borders of business. Addressing security concerns must be balanced with taking a user privacy-centric approach to ensure a strong security culture across your organization. Enterprises need to quickly move to a more holistic approach to data protection and reduce their overall risk. This means extending data protection across all aspects of a business: people, processes, training, and tools.

Initially, Microsoft's own approach to insider risk was fragmented, with our security teams often siloed from other organizations and where end-user training on data protection strategy was less frequent or robust. From the role of a Chief Information Security Officer (CISO), who's responsible for data protection and ensuring the security of your corporate assets, we recognized the importance of insider risk management and made internal changes that aimed to take a comprehensive approach to addressing potential insider risks like data theft, data leakage or unauthorized access of sensitive data.

We did this by shifting our mindset on insider risk from focusing solely on risk management to thinking about creating value and building a stronger security culture across our organization. This included building an organization-wide cybersecurity culture through corporate trainings and a great emphasis on user stewardship of corporate data, ensuring that trust remains foundational to our company approach and our products, and building a solution that helps us to detect and respond to insider data security risks like data leakage and data exfiltration while protecting user privacy and leveraging strong security controls, which has since evolved into our Microsoft Purview Insider Risk Management solution.

As Microsoft's CISO, I work hand-in-hand with other leaders across Compliance, Corporate, External and Legal Affairs, Human Resources and Product Engineering to make sure that we are addressing insider risks in a way that meets our security needs while also continuing to build employee trust.

At Microsoft, we are constantly looking to do better for our own security practices, as well as offer security guidance that other organizations and security teams may find helpful in their own security journeys.

The content in this report is to help security and compliance leaders think about how they approach data protection and insider risk management within their organizations. This report lays out a number of new findings about how organizations can go from a "fragmented" approach to insider risk management to a "holistic" one, addressing potential risks from multiple lenses, with cross-leadership buy-in and as part of a greater data protection strategy. For example, we found that more than 90% of holistic organizations believe privacy controls should be used in the early stages of investigations. Holistic organizations also get more buy-in on their risk programs from other departments, like legal, HR, or compliance teams, which is critical to building a culture of security. Finally, holistic organizations agreed that "training and education are vital to proactively address and reduce insider risks," compared with 50% of fragmented organizations.

We recognize that tools are just a part of your data protection strategy - it must also include the right people, processes, and training/education in place to be effective. The report also shares best practices for organizations who endeavor to approach insider risk management more holistically, and build a program that fosters trust, empowers users, and makes privacy a priority.

---

[1] *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025*

Executive summary

The exponential rise of remote and hybrid work, along with digital data proliferation, has brought on an increasing level of concern surrounding insider risks. Organizations around the globe face real challenges in protecting themselves from harm—both inadvertent and malicious—arising from misuse of authorized access. But just as important, how do they implement programs that preserve trust and a positive company culture?

This paper details the survey results of 300 security and compliance professionals from across the United States to create a richer picture of the challenges they're facing around insider risk, the current state of their insider risk programs, and the key elements of their programs that are yielding positive results. The report also features recommended best practices for security leaders regardless of where they are in their own insider risk program journeys. The main questions that this Microsoft-commissioned study sought to answer were:

Which elements best characterize success in an insider risk program? And where should programs look to grow and advance?

The survey found a strong connection among companies with relatively greater insider risk management success and their responses to questions related to how holistic their programs are.

From this insight, we developed a continuum in which we placed organizations on the degree to which they believe in and manage programs either more or less holistically, taking into account the right people, processes, training and tools to manage insider risk. We call this the Holistic Insider Risk Management Index (HIRMI). We identified a consistent pattern of attitudes, behaviors, and outcomes among companies and scored them against one of the following areas on the index: holistic (high), evolving (middle), and fragmented (low). We also identified key areas that organizations should be thinking about to better align their insider risk management programs to be more holistic.

Respondents who ranked higher on the HIRMI model tended to focus more on creating a stronger company culture through a holistic approach. They engaged in a more proactive and meaningful way with employees and scored higher on

importance and concern for trust, privacy, productivity, and organizational buy-in.

Programs that ranked higher on the HIRMI model are also more likely to place an emphasis on positive deterrents. They attribute their success, in part, to effective employee training, and view strong employer-employee relationships and organizational support as vital to insider risk management. More holistic programs strive to involve more departments in insider risk management programs, recognize the importance of needs-based tools, and detect potential insider risk events faster.

While it appears that developing a more holistic program is good for employee morale, does it also result in better insider risk outcomes for an organization?

Our goal is to share findings with organizations looking for ways to improve, maximize, or even establish an insider risk program. This paper aims to help any company—regardless of its positioning on the HIRMI—prepare for and mitigate insider risk.

Table of Contents

The growing problem of insider risk

The COVID-19 pandemic drastically disrupted work life worldwide. Almost overnight, the percentage of employees working remotely grew exponentially and fundamentally shifted where and when employees work and how they gain access to company networks.

Microsoft's Work Trend Index 2022[2] found that hybrid work is up to 38% and that 53% of people are likely to consider transitioning to hybrid in the year ahead. Those figures align with the digital trend that's evolved over the last decade, making it easier it easier for individuals to collaborate across across offices and remote locations.

This increase in remote and hybrid work has led to growing concern about insider risk incidents. Two-thirds of our study respondents highly agreed that, ***"Data theft or data destruction from departing employees is a form of insider risk that is becoming more commonplace."***

The occurrence of insider risk events can vary widely from company to company, with our respondents indicating the average number of inadvertent events they identified was around 12 per year, or once per month. Malicious events happened at a slower pace, with close to eight events per year. This is an average of 20 events per year across all industries. While only one-third of respondents reported their insider risk event occurrence increased in the past year, *a majority (40%) expect events to increase moving forward.*

Many organizations are looking for ways to better manage insider risks, while also supporting their employees and fostering a culture of trust. Having to respond to frequent escalations can send some companies to extremes, including an "always on" or overly proactive approach that continuously checks on their employees. This risks eroding employee trust and productivity and can put security teams at odds with other leaders in an organization. But the abandonment of all insider risk mitigation efforts can expose the company to severe if not existential data security risks.

Experts on insider risk at the Carnegie Mellon CyLab institute repeatedly show that a balance must be struck. "Workforce management practices that bolster perceived organizational support serve to improve employees' organizational commitment in a way that complements traditional security practices to provide a more holistic risk management balance."[3]

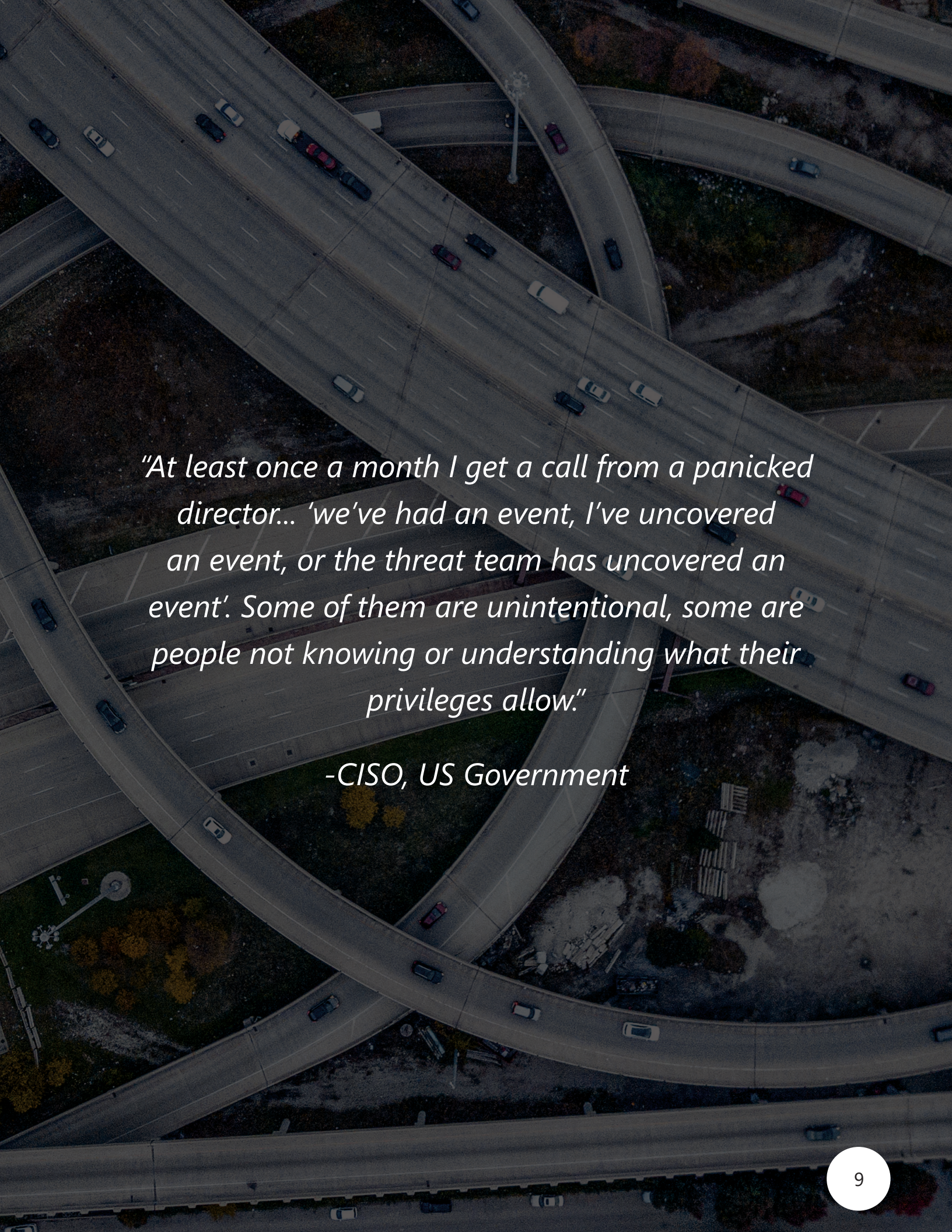
Our study also showed that supportive practices from organizations, like training and stronger feedback loops, resulted in positive impacts on insider risk management.

These supportive practices become even more important in the hybrid work environment as a means of fostering connectivity across a disconnected work populace, which in turn can potentially help mitigate insider risk.

---

[2]*Microsoft Work Trend Index 2022. "Great Expectations: Making Hybrid Work Work"*

[3]*CyLab at Carnegie Mellon University. (2021) Insider Risk Management Program Building: Results from a Survey of Practitioners [white paper].*



"At least once a month I get a call from a panicked director… 'we've had an event, I've uncovered an event, or the threat team has uncovered an event'. Some of them are unintentional, some are people not knowing or understanding what their privileges allow."

-CISO, US Government

Defining insider risk

Before delving into the details of our findings, let's review some basic definitions.

What is insider risk?
For the purposes of this paper, insider risk is defined as the potential for a person to use authorized access to the organization's assets—either maliciously or unintentionally—in a way that negatively affects the organization. Access includes both physical and virtual (cyber) access; assets include information, processes, systems, and facilities.

What is insider risk management?
In the study, we define insider risk management as activities intended to detect and/or prevent a person from using authorized access to the organization's assets—either maliciously or unintentionally—in a way that negatively affects the organization. These activities can be performed in a formally coordinated manner, as part of a centralized program, or more informally outside of an organized program or structure.

What are common types of insider risk?
There are two main types of insider risk that we focused on for this study: inadvertent and malicious. While malicious cases—including fraud, IP theft, and even corporate espionage—are perhaps what first come to mind when the topic of insider risk arises, inadvertent cases—which can include an employee unknowingly taking unsafe actions—are more common by far.

Malicious cases, while less common, can be more costly. We'll look at results regarding both types of instances later in the paper.

Inadvertent

An employee unintentionally causes harm. This can occur when an employee:

- Takes unsafe actions
- Is untrained or distracted
- Misuses resources
- Causes other accidental data leakage

Malicious

An employee sets out to cause harm, such as:

- Fraud
- IP theft
- Unauthorized disclosure
- Sabotage
- Corporate espionage

"We have found [inadvertent access]…it gets reported, it goes to Compliance, and they review what, why, and how … Everything's happened, from a slap on the wrist to an immediate termination, depending on the circumstances around it. "

-CTO, Healthcare Services

The cost and challenges of insider risk… it's not just financial

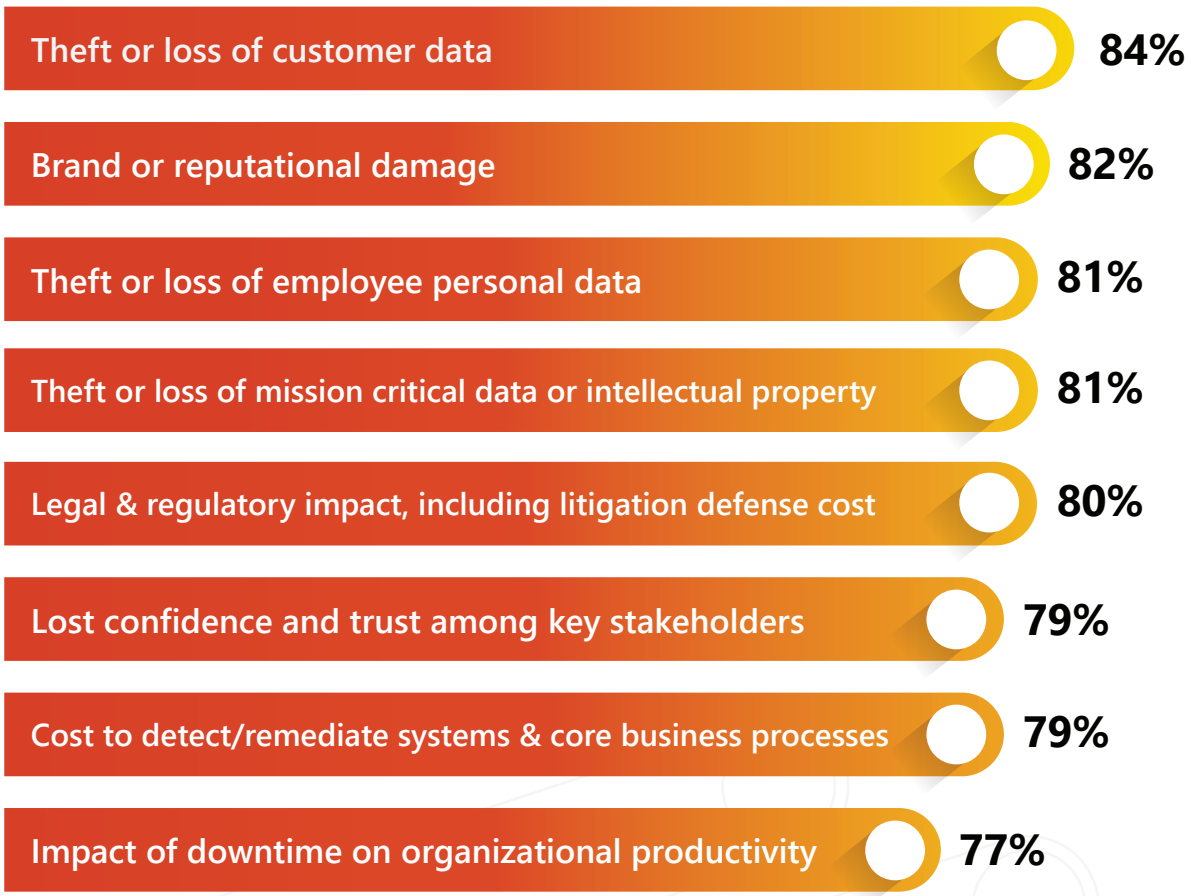
Beyond the wider challenges of shifting work environments and remote and flexible work mentioned earlier, we wanted to better understand the cost of insider risk to organizations and challenges they face in creating programs to protect against it.

Loss of data and trust

When we asked respondents to answer what the greatest potential impact insider risk had on their organization, ***loss of customer data and damage to brand or reputation*** topped the list.

We asked respondents to rate the relative magnitude of impact to their organization from insider risk events. The highest-rated impacts at 84% were from theft or loss of customer data, followed closely by damage to brand or reputation at 82%. Other types of highly rated, impactful insider risk events included theft or loss of employee personal data, mission critical data, or intellectual property, as well as legal or regulatory impacts and loss of confidence and trust among key stakeholders.

Figure 1: Highest-rated impacts of insider risk events on the organization



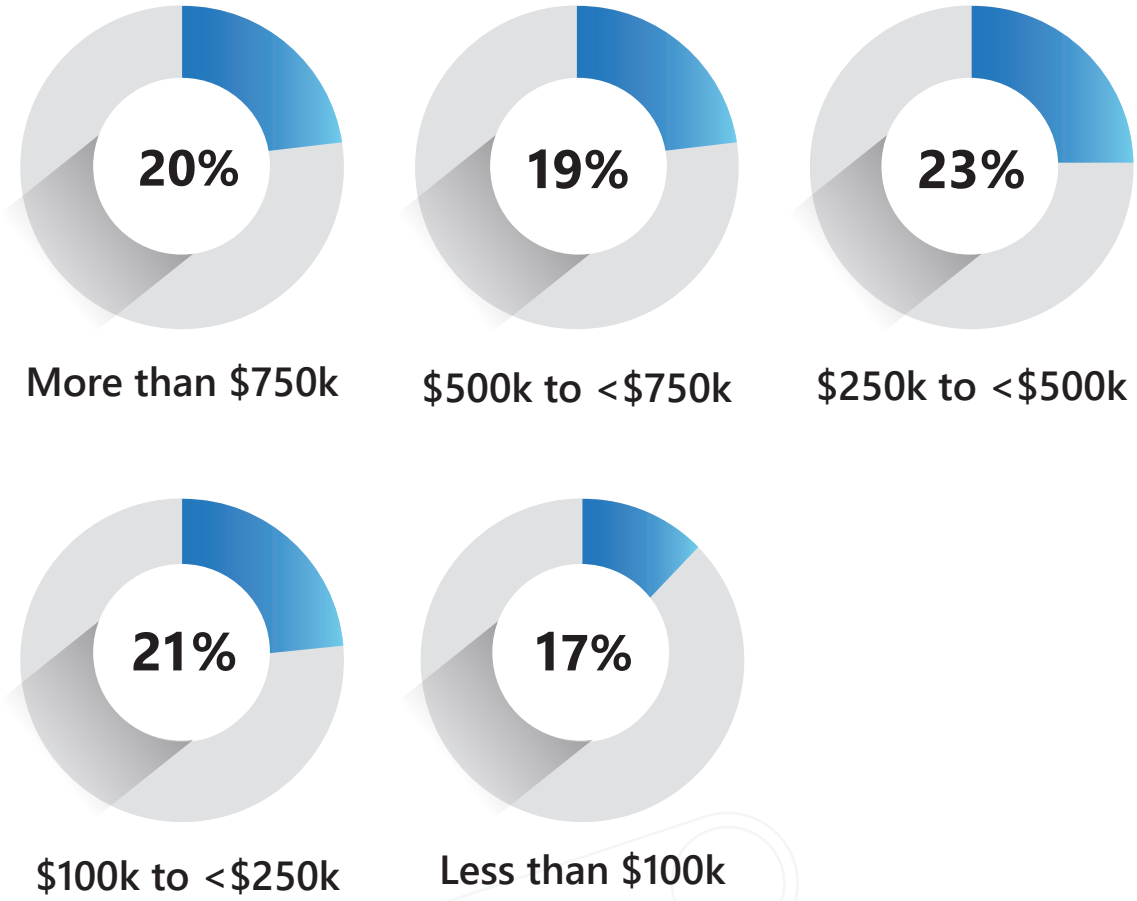
Monetary cost

When asked to estimate the average monetary impact of a single data breach from an insider event, ***almost 40% of respondents said the average cost was more than $500,000 for a single event***, with an average of 20 events per year. This study included respondents from small- and medium-sized businesses, as well as large enterprises, for whom the average cost per incident could be far greater.

When calculating the average number of insider risk incidents per year, a company can expect costs in the millions on an annual basis. These average estimates are likely on the lower end of the cost spectrum and, when including other factors such as loss of brand reputation and trust, costs can quickly escalate.

For example, in 2021, after a chemist in the U.S. was granted access to company secrets from her employers, The Coca-Cola Company, and Eastman Chemical Company, she was convicted of conspiracy to steal trade secrets, economic espionage, and wire fraud. The development cost of those stolen trade secrets was nearly USD $120,000,000.[4]

Figure 2: Average cost of one insider risk data breach



[4]*U.S. Department of Justice (2021). Ph.D. Chemist Convicted of Conspiracy*

Insider risk management program challenges

Degradation of trust in the work environment

The impact of insider risk events can be substantial, as can the impact from the steps required to mitigate insider risk events.

The potential negative consequences of insider risk management programs further illustrate the need for a holistic approach.

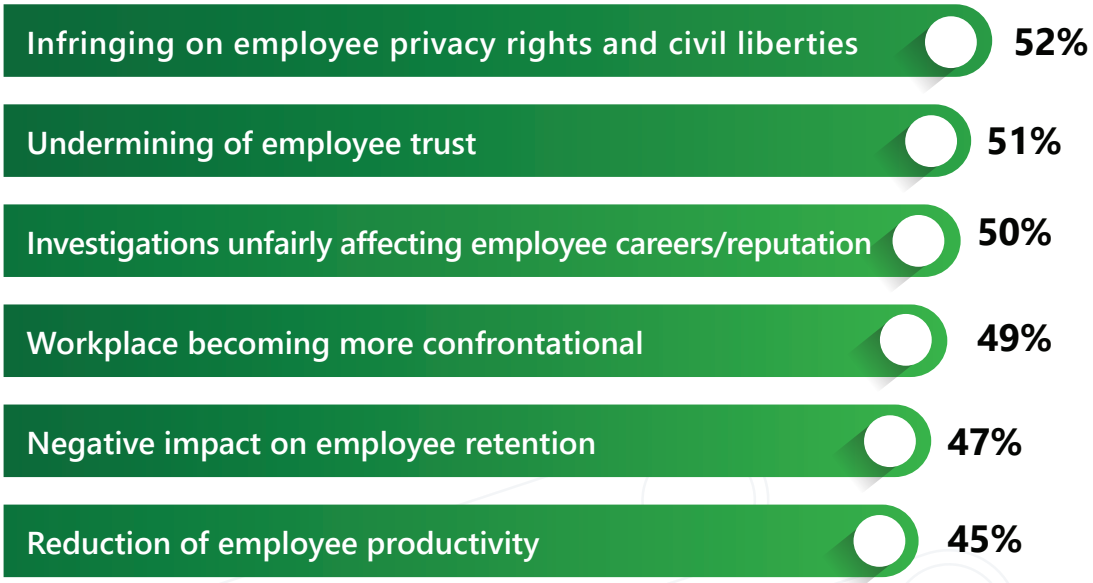
Many organizations point to concerns over employee privacy rights (52%), loss of employee trust (51%), and general degradation of the working environment when considering their insider risk programs—all areas that can be mitigated by a more balanced insider risk management approach.

Companies concerned about employee retention should prepare for possible pushback and misunderstanding, especially around policies that might impact an employee's day-to-day activities. To mitigate these issues, companies that feel they have more successful programs use education, training, and awareness as means to explain the need for data security policies.

Hiring and retaining dependable personnel

Another interesting challenge for insider risk programs is to ensure that the people who are most likely to abuse or leak data are not themselves responsible for investigating potential insider risks. We asked respondents to rate the level of risk

Figure 3: Areas of high concern around negative consequences from insider risk programs

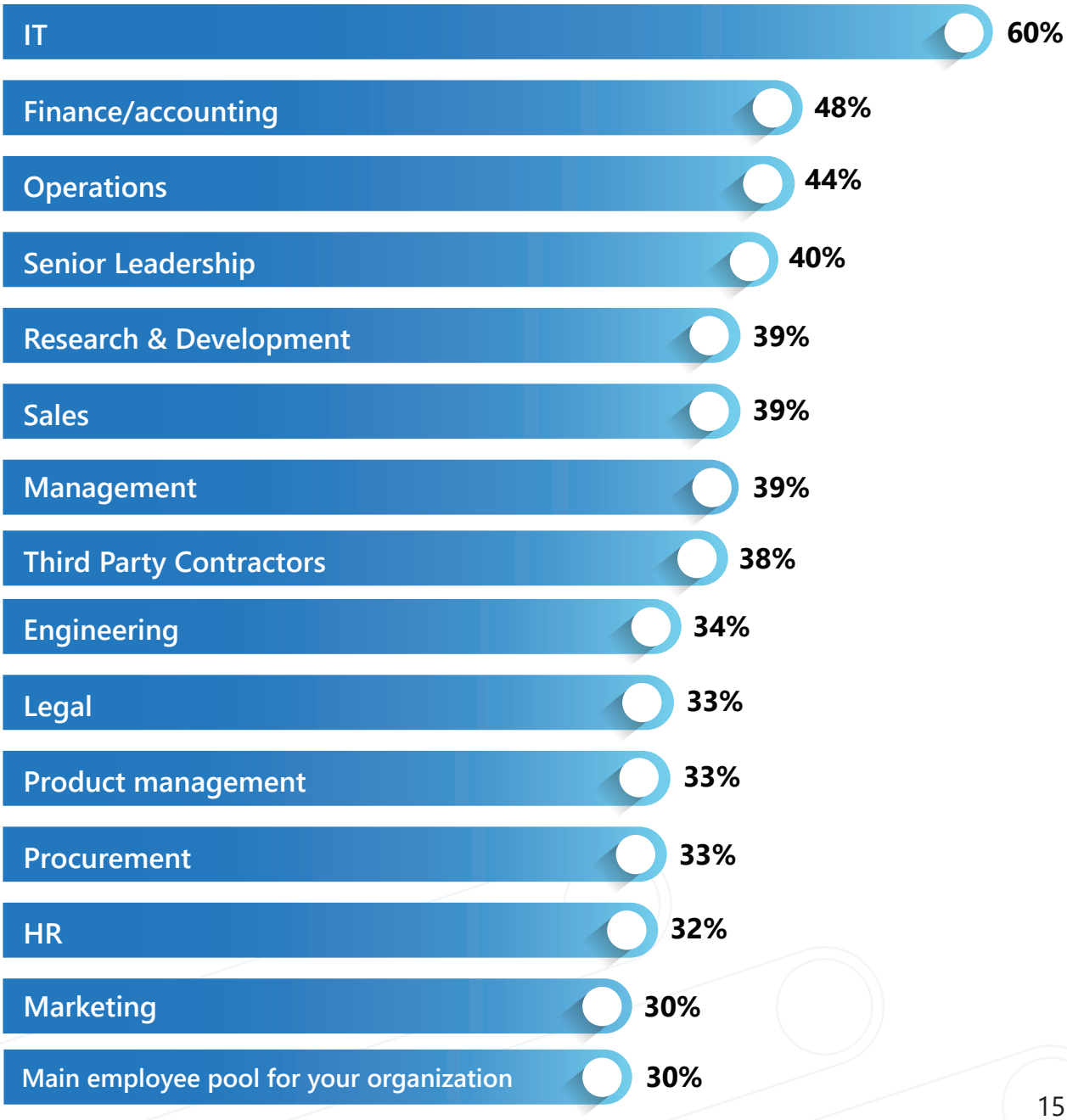


they associate with various departments and business groups. Surprisingly, IT—the department most often tasked with detecting and remediating insider risk—is also the department most commonly associated with being at risk for this very issue, with 60% seeing it highly at risk.

Finding reliable personnel you can trust to complete the job of insider risk detection and remediation is one of the challenges to running a successful insider risk management program.

This makes it all the more important to ensure that the security and IT teams investigating insider risks have strong auditing and approval controls in place, to make sure that their actions are in the best interest of the organization.

Figure 4: Level on insider risk associated with different departments



So, which insider risk approaches are most comprehensive?

What is the proper mix of elements for an insider risk management program? Who should be involved? How does a company help mitigate the employment stressors on employees' lives that might lead to disgruntled employees? What kind of deterrents should be considered and prioritized? How important is training, education, and communication about the program?

It's a complicated subject that deals with multiple elements. The qualitative and quantitative research conducted by our team set out to answer these questions and to provide a better understanding of the challenges security professionals are facing in the realm of insider risk and how they are addressing those challenges.

During this process, we were able to identify companies addressing insider risk more comprehensively, the approach they're using, and what they're doing differently than others. We discerned the necessary elements, tools, and processes they have in place.

Deterrents
Throughout the paper, we will often refer to the terms *positive* and *negative* deterrents. Let's explain what we mean:

Positive deterrents are proactive measures to mitigate the likelihood of insider events, including employee-morale events, more thorough onboarding, ongoing data security training and education, upward feedback, and work-life balance programs. Positive deterrents engage in a productive and preemptive way with the source of risk: its employees.

Negative deterrents are practices that check on and constrain employee behavior. This can be through the use of tools and solutions broadly that block users from engaging with, accessing or sharing content, thereby creating a more reactive environment in contrast to the proactive emphasis of positive deterrents.

[5]*A. P. Moore, T. M. Cassidy, M. C. Theis, D. Bauer, D. M. Rousseau and S. B. Moore, "Balancing Organizational Incentives to Counter Insider Threat," 2018 IEEE Security and Privacy Workshops (SPW), 2018, pp. 237-246, doi: 10.1109/SPW.2018.00039.*

"An insider threat program that balances organizational incentives can become an advocate for the workforce and a means for improving employee work life—a welcome message to employees who feel threatened by programs focused on discovering insider wrongdoing."[5]

From IEEE report – "Balancing Organizational Incentives to Counter Insider Threat"

Key elements of the Holistic Insider Risk Management Index

For this study, we developed the Holistic Insider Risk Management Index (HIRMI), which measures how holistic an insider risk management program is based on measurements related to the integration of the following four categories: **people, process, tools, and training**. We measured respondents' agreement with the importance and usage of:

PEOPLE: Cross-organizational buy-in

PROCESS: A balanced approach to insider risk

TOOLS: Ability to have integrated tools and technology suitable to address insider risk management needs

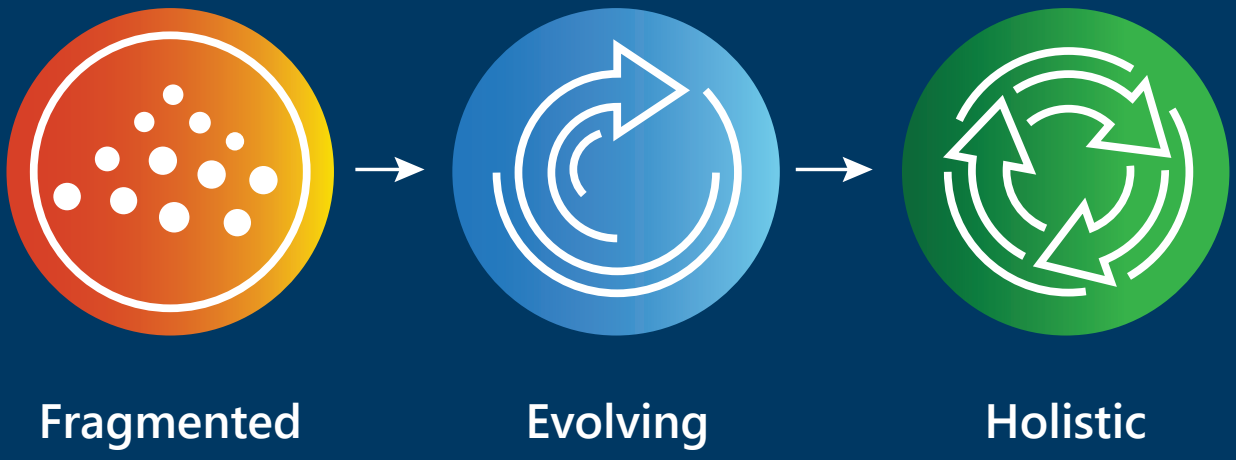
TRAINING: Effectiveness of insider risk training

Our index looked at the current state of how companies are addressing these elements with their insider risk programs. We specifically looked for any discernable differences among companies and how they approach insider risk. The index is inspired by a recent study from CyLab at Carnegie Mellon University that concurred with three of our four key HIRMI elements *(people, process, and tools)* as beneficial to an effective insider risk program.[6]

The more people focused on and addressed these four elements, the more holistically they were approaching insider risk. And, to a certain degree, the holistic approach to insider risk influences the very culture of the organization.

[6]*CyLab at Carnegie Mellon University. (2021) Insider Risk Management Program Building: Results from a Survey of Practitioners [white paper].*

Figure 5: HIRMI profiles



HIRMI profiles

As we assessed our findings, we began to see three distinct profiles emerge around how firms approach insider risk. These profiles aligned with particular attitudes, behaviors, and outcomes, as follows:

Assess yourself: Based on our HIRMI definitions, which model best describes your organization?

Fragmented
(31% of sample)

- Recognize the need for an insider risk program and might already have one or are building toward it, but might be misaligned on success measures
- See value in positive deterrents that reduce risk but have low current usage
- Believe they understand what's required to lower insider risk, but do not commit resources or gain company-wide buy-in

And are more likely to:

- De-prioritize employee and employer relationships or cross-organizational buy-in for an insider risk program
- Use fewer positive-deterrent programs (using two or fewer in many cases)
- Expect events to decrease in the coming year

Evolving
(40% of sample)

- Realize the importance of employees to an insider risk program, but might need to place greater emphasis on improving the work environment
- Recognize their program can include more buy-in, tools, and training
- Demonstrate cost-consciousness that can outweigh concerns for privacy

And are more likely to:

- Feel less concerned about insider risk impacting employee productivity
- See greater impact from legal and regulatory costs and might worry more about program costs
- Expect inadvertent events to increase significantly in upcoming year

Holistic
(29% of sample)

- Approach insider risk with a comprehensive attitude to examine all facets of what an insider risk program could include
- Encourage company-wide integration and involvement
- Believe that employee-employer relationships are key to reducing the likelihood of insider risk incidents

And are more likely to:

- Express significantly higher sensitivity for employee productivity, privacy, and trust
- Hold more frequent employee training
- Detect events faster and flag more for investigation

"As far as cost and reduction in productivity, my feeling and my direction is always how can I minimize that as much as possible while still having that visibility?"

-CISO, US Government

5 key characteristics of holistic insider risk management

"Organizations want to rush into an insider risk management program when they don't have the basics down."
-CISO, Financial Services

When measuring the success of an insider risk management program, some organizations place an emphasis on reducing false positives as a means of increasing success. Of course, fewer false positives are beneficial, but several other factors are vital to a successful program, including maintaining positive relationships with your employees, incorporating buy-in about data security across the organization, and using efficient tools.

Organizations that address insider risk in a holistic manner—which includes the process, people, tools, and education involved in an insider risk management program—perceive themselves to be successful and sophisticated.

We assert that the more firms deal holistically with the issue of insider risk, the more effective they are at addressing it.

Holistic organizations are more likely to display the following characteristics:

1 Prioritize employee trust, productivity, and privacy controls

Holistic organizations prioritize employee employer relationships and integrate privacy controls and policies in their programs to maintain—and even boost trust. Around 89% of these companies expect to increase privacy controls in their programs in the coming year.

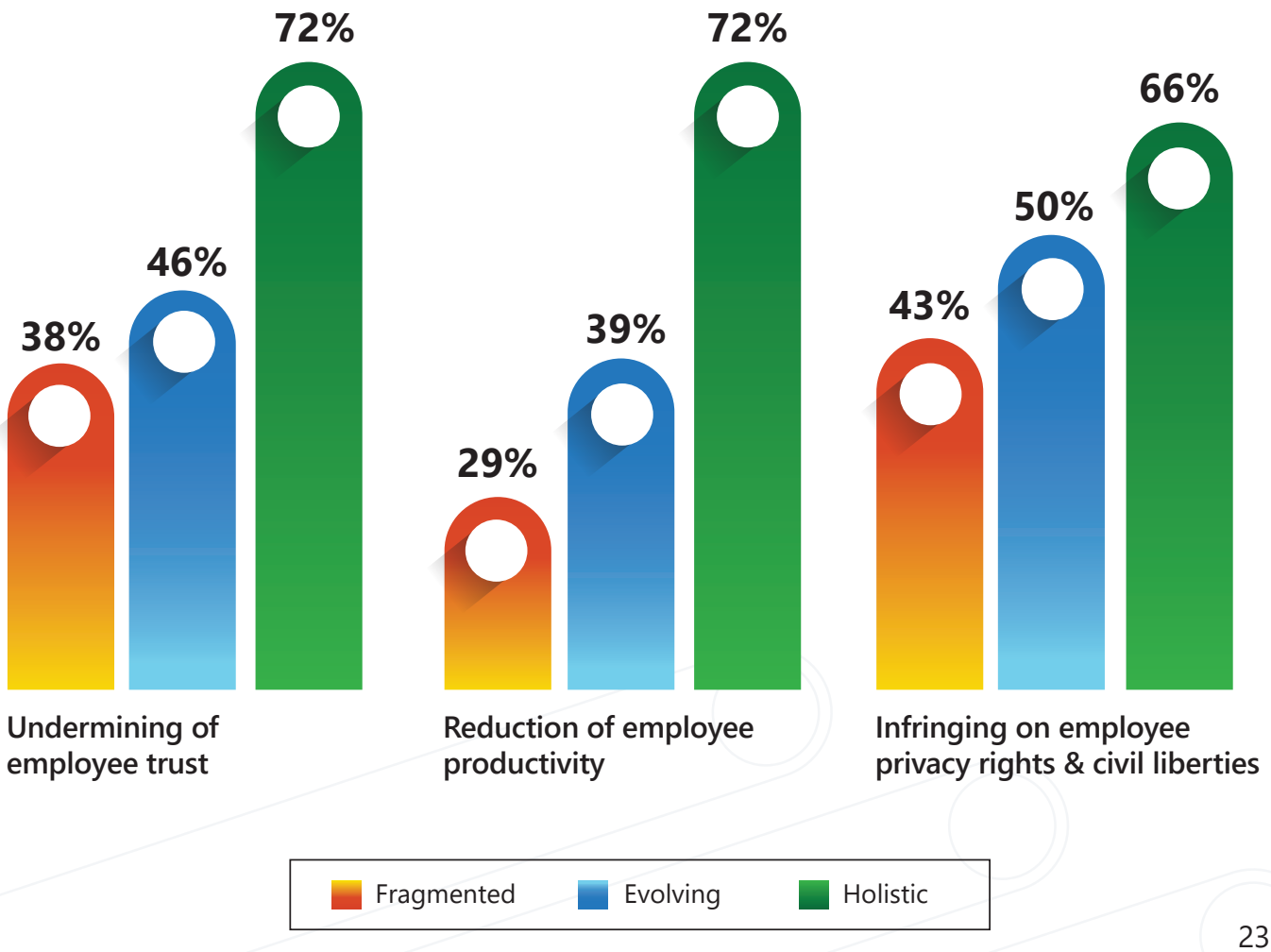
We found that ***94% of the holistic companies with which we spoke noted that a key element to program success is finding a balance between employee privacy and company security.***

Figure 6: Designated importance placed on balancing employee privacy with company security

Holistic organizations ***ranked higher in their concern about the potential negative consequences of insider risk management programs, such as undermining employee trust, at nearly 72%*** (vs. 46% in evolving and 38% in fragmented firms) and ***infringing on employee privacy rights and civil liberties, at nearly 66%*** (as compared to nearly 50% in evolving and 43% in fragmented organizations).

Concerns around productivity also feature prominently among holistic organizations. As zero-trust strategies grow in popularity, more constrained access and verification steps can put employee productivity at risk. A holistic approach that incorporates transparency and employee engagement around data risk can help ease any hit to productivity.

Figure 7: Level of concern for negative consequences of insider risk management programs



Establishing privacy controls also builds employee confidence

Creating and setting up privacy controls that protect an employee's identity during investigations helps reduce the tension and anxiety created by insider risk management programs. It also helps build and maintain trust throughout the organization. We found that holistic companies have more privacy controls in place and put greater emphasis on the importance of trust.

More than 90% of holistic organizations agree that privacy controls should be used in the early stages of investigations, while only 44% of fragmented companies agree. Holistic companies are more likely to employ user pseudonymization (replacing personally identifiable information, like the name of the user, with a pseudonym) as a key tool to reduce the potential for privacy issues during false-positive events.

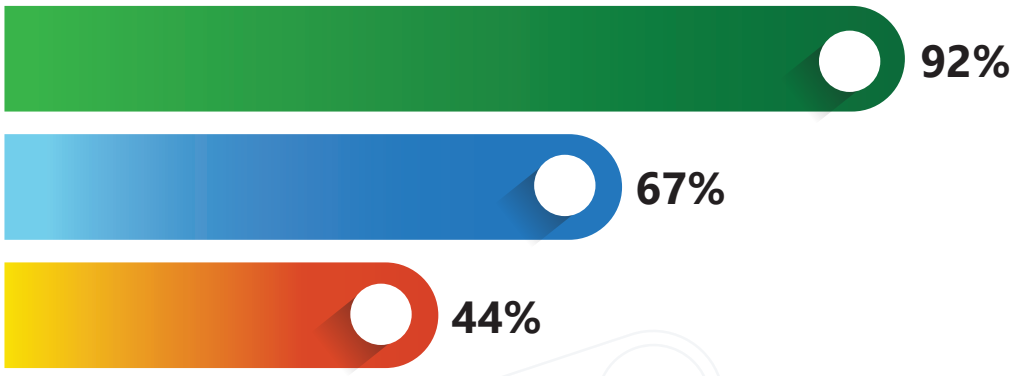
Figure 9 shows additional privacy controls organizations can implement. We see a significantly higher level of privacy controls used in holistic companies compared with fragmented and evolving ones. A higher portion of fragmented companies also have no future plans to implement these types of controls.

Evolving firms are actively growing their privacy-related policies and rules for their programs with increasing usage of multiple levels of approval and role-based access controls. (Figure 9)

We also found the number of controls used is a differentiating factor along the HIRMI.

Fragmented companies are more likely to have two or fewer of these privacy controls in place, such as additional auditing into the activities of the investigators and deletion of investigation flags after a period of time. (Figure 10)

Figure 8: Agreement with employee privacy in the early stages of an insider risk investigation



It is critical that a user's identity is protected during the early stages of an insider risk investigation

Figure 9: Privacy controls currently in use

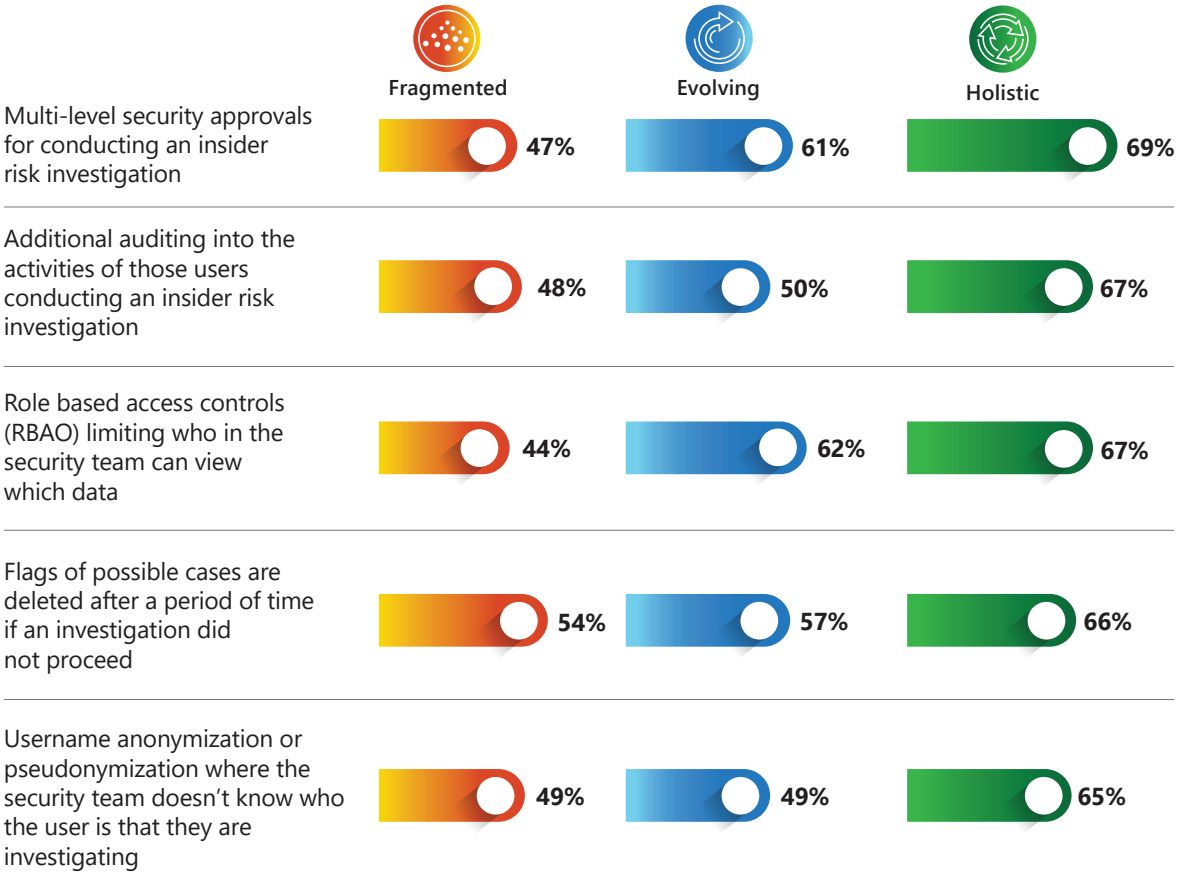
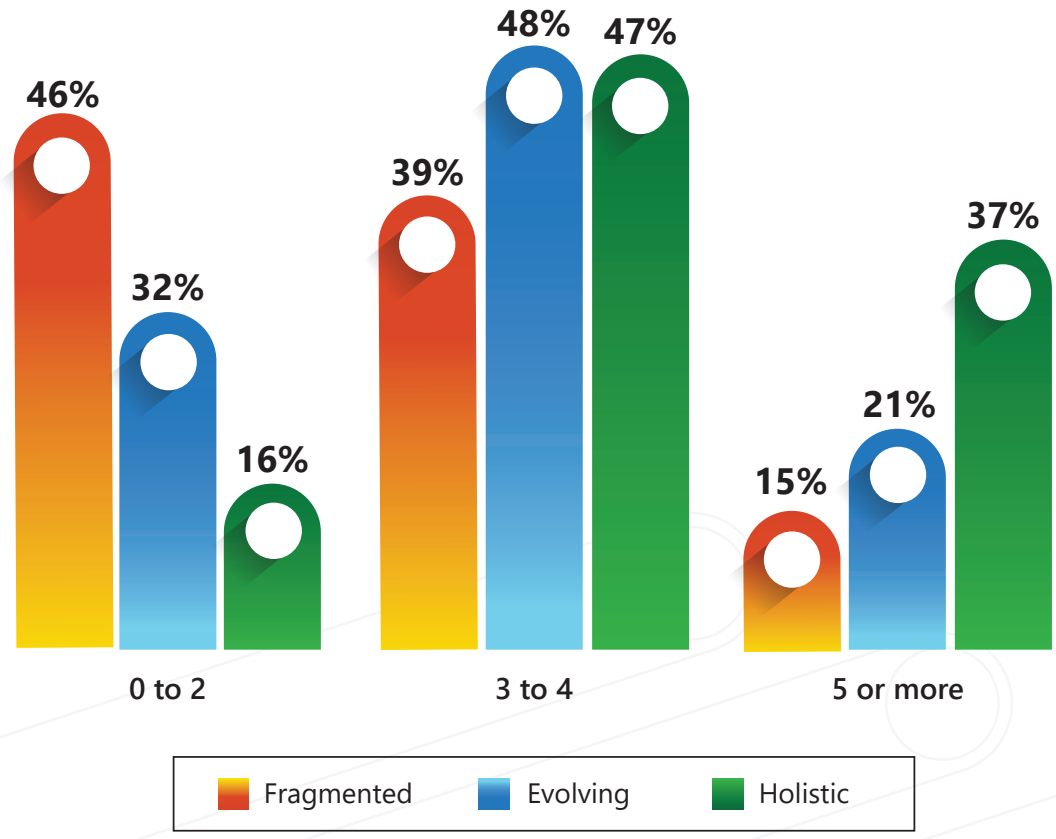


Figure 10: Number of privacy controls currently in use



2 Attain program buy-in and involvement across the organization

Companies with more developed holistic insider risk management programs typically have more buy-in and involvement in the program throughout the organization. We observed a clear connection between an increase in the breadth and depth of involvement among different departments and the program's holistic approach.

Starting an insider risk management program has its challenges, and getting and maintaining buy-in is one that persists. The more all parts of the organization are engaged, the easier it will be to detect and remediate insider risk events and secure funding for the program.

IT and security groups will always lead the way for high involvement and buy-in, as we can see in Figure 11.

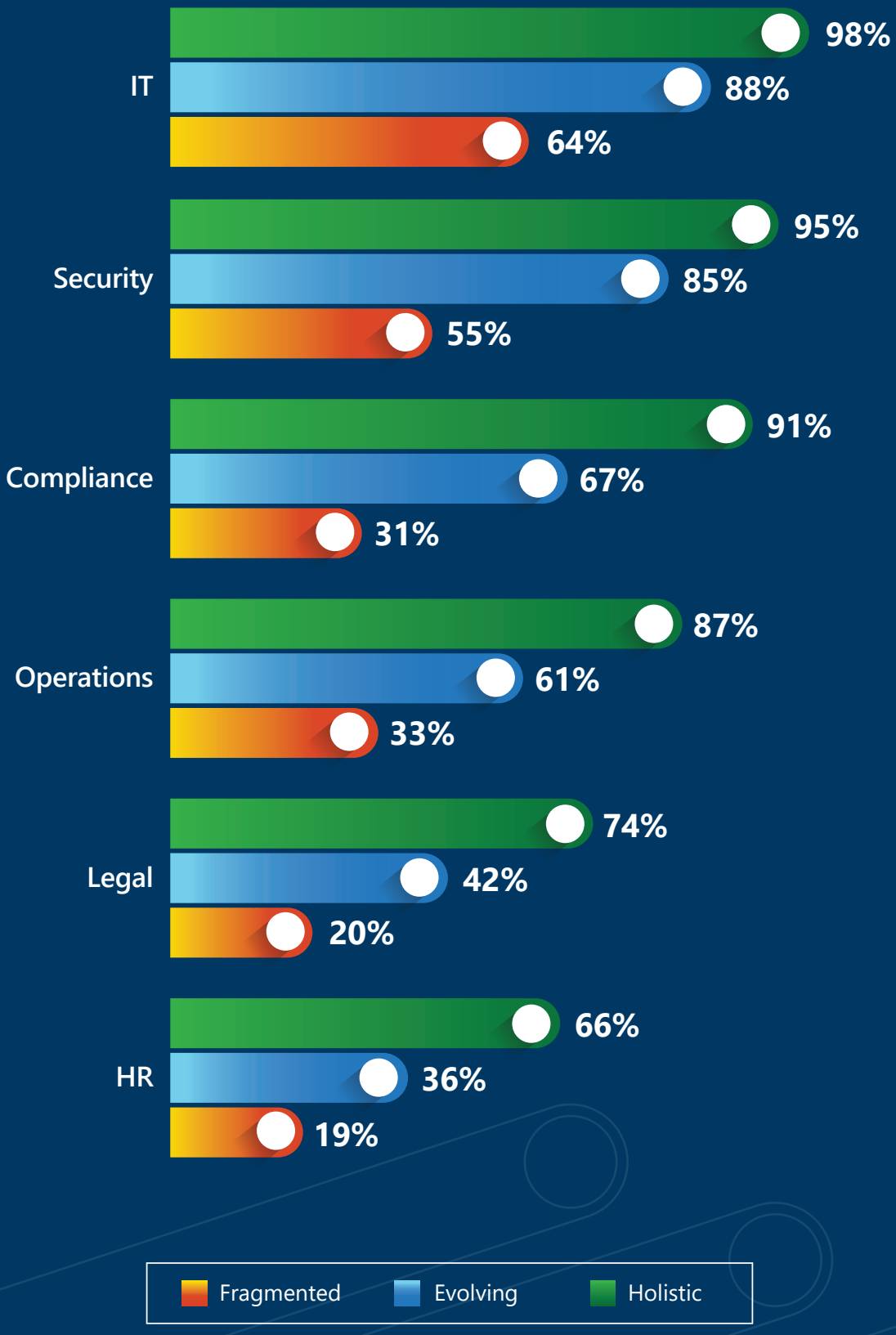
What's even more revealing is the drop-off of highly involved departments after IT and security. Among fragmented companies, the drop-off happens immediately after IT and security, whereas with evolving companies we see compliance and operations departments being more highly involved, in addition to IT and security, but dropping off after that.

With holistic companies, we see the higher likelihood of all key departments being involved—pointing to a greater level of buy-in across the organization. Compliance, legal, and human resources departments can provide additional perspectives and support within their fields. For example, including human resources stakeholders can be critical with respect to measure of company culture and landing positive deterrents such as training.

"[Insider risk] is a business problem so you have to think about the business outcome as the product of what you're doing. So, the folks that should be involved are, first and foremost, legal, human resources, and the business units. Those are the three usual suspects that need to be part of the conversation."

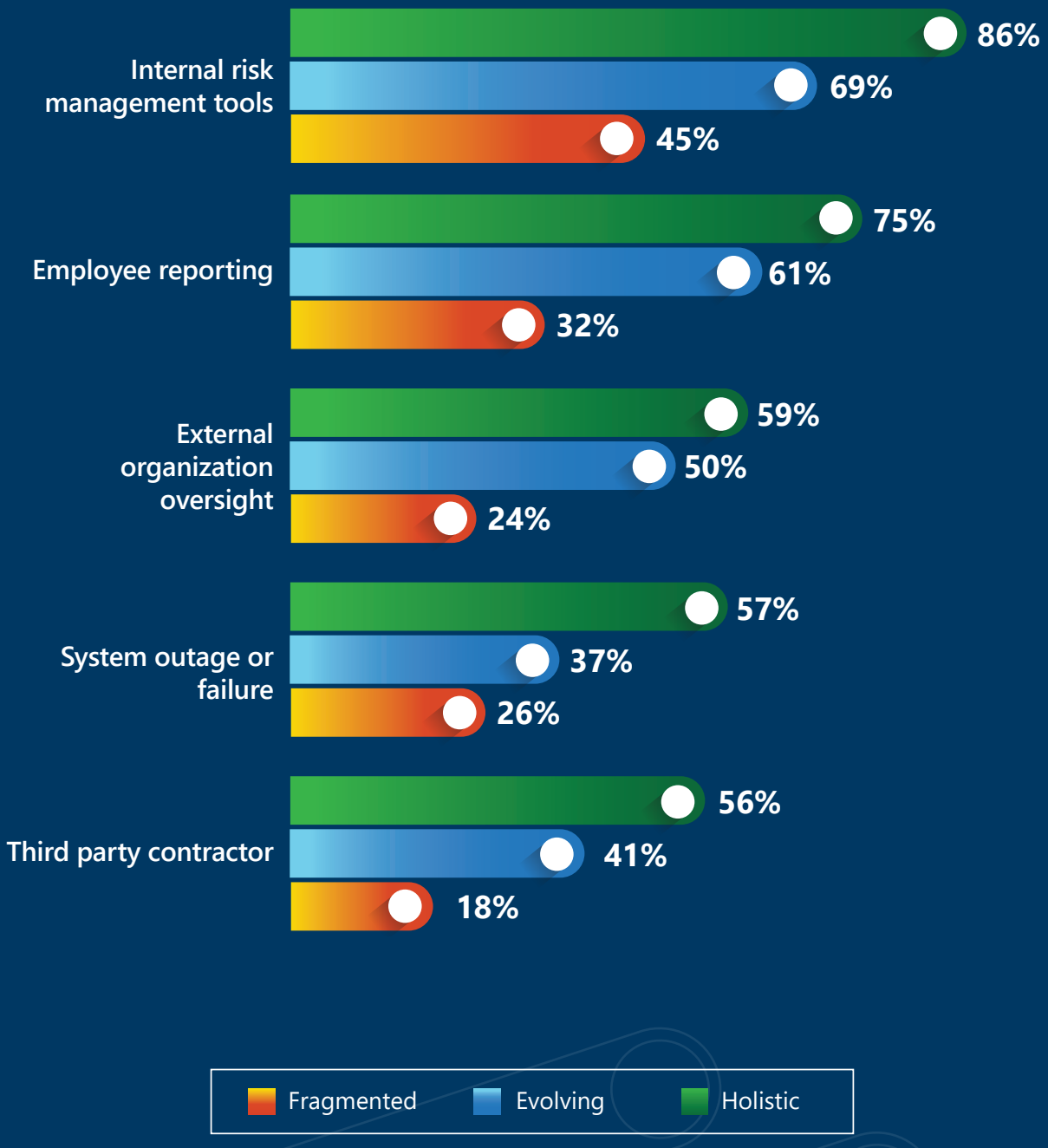
- CISO, Financial Services

Figure 11: Departmental level of high involvement with insider risk management



Furthermore, among holistic organizations, our findings show it's significantly more common for employee reporting to be a method of detecting insider risk events compared with fragmented programs. This is another form of increased buy-in we see for holistic organizations. Their employees now become potential assets to help mitigate events and further spread awareness.

Figure 11a: Level of usage for common methods of insider risk event detection



"You have to try to bring your people along for the journey. You'd be surprised how often a vigilant and aware team member or employee can really help you get in front of things very quickly."

CISO, Financial Services

3 Attest that effective training and education are vital

Holistic organizations consider employee data security training and education critical to a successful insider risk management program. By improving data security education and training, holistic companies can then rely more on employees as a first line of defense complemented by a strong backing of detection tools.

Effective training and education on proper data security and protection is a differentiator in obtaining employee buy-in. Organizations that detail the importance and impact of insider risk events on the company, employees, and job security can help justify the steps being taken to mitigate risk. They evangelize the program and increase awareness around events such as protecting sensitive information from going to competitors, inappropriate data leaks, or inadvertent data sharing.

Holistic firms recognize this need more than fragmented organizations, as we see in Figure 12.

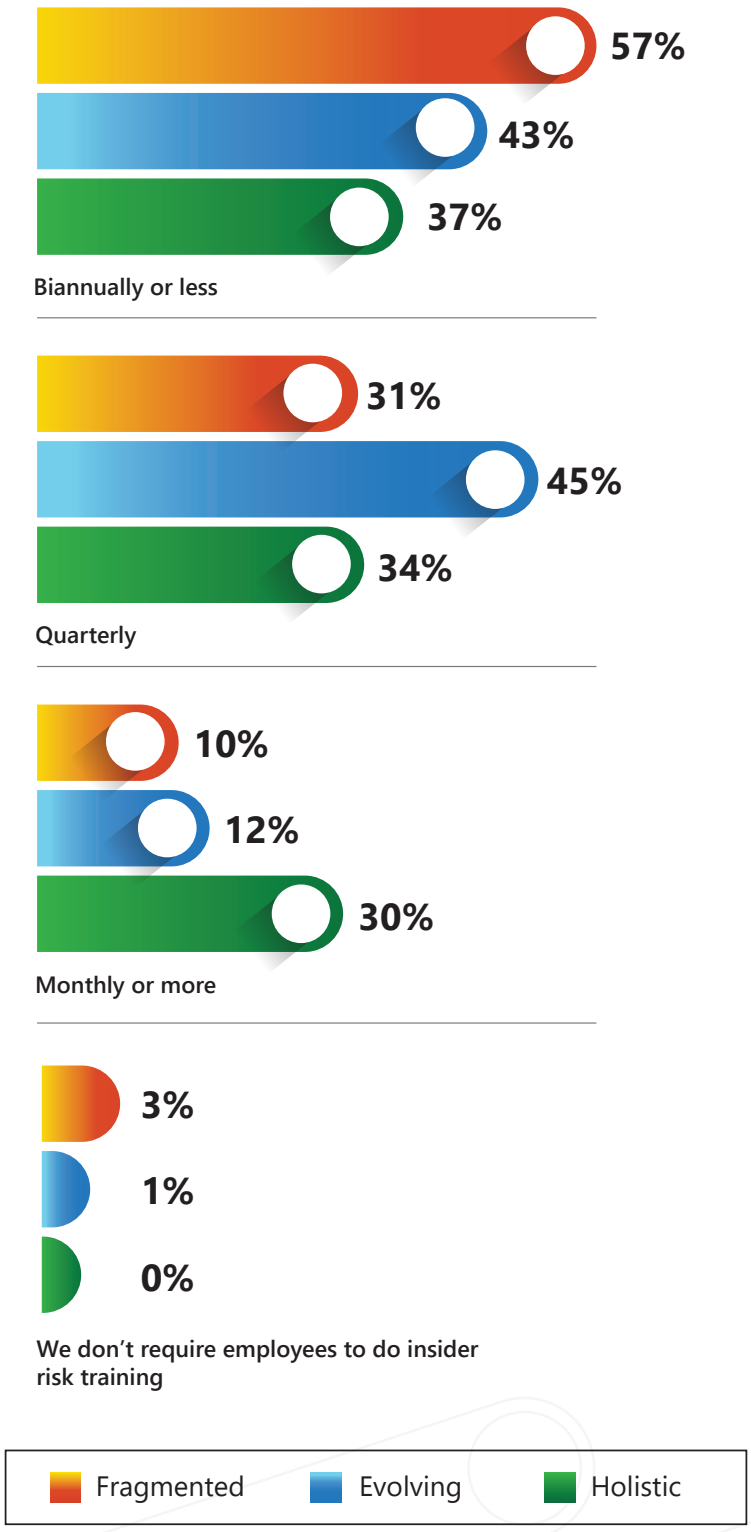
Frequency of training impacts effectiveness

Getting employees to sit through—and meaningfully engage with—data protection and compliance training education can be challenging, but repetition works. Holistic companies conduct more training than fragmented ones, and in doing so, provide opportunities for employees to better understand how they can be part of mitigating data security risk and why it's important to do so. Some respondents indicated that they preferred shorter but more frequent trainings. (See page 28 for figure 13)

> "I send out little [training] reminders with short explanations because if I write a long explanation, nobody will read it anyway."
>
> - VP IT, Healthcare Services

Figure 12: Level of importance and agreement about the impact of training and education on insider risk management

Figure 13: Frequency of training and education

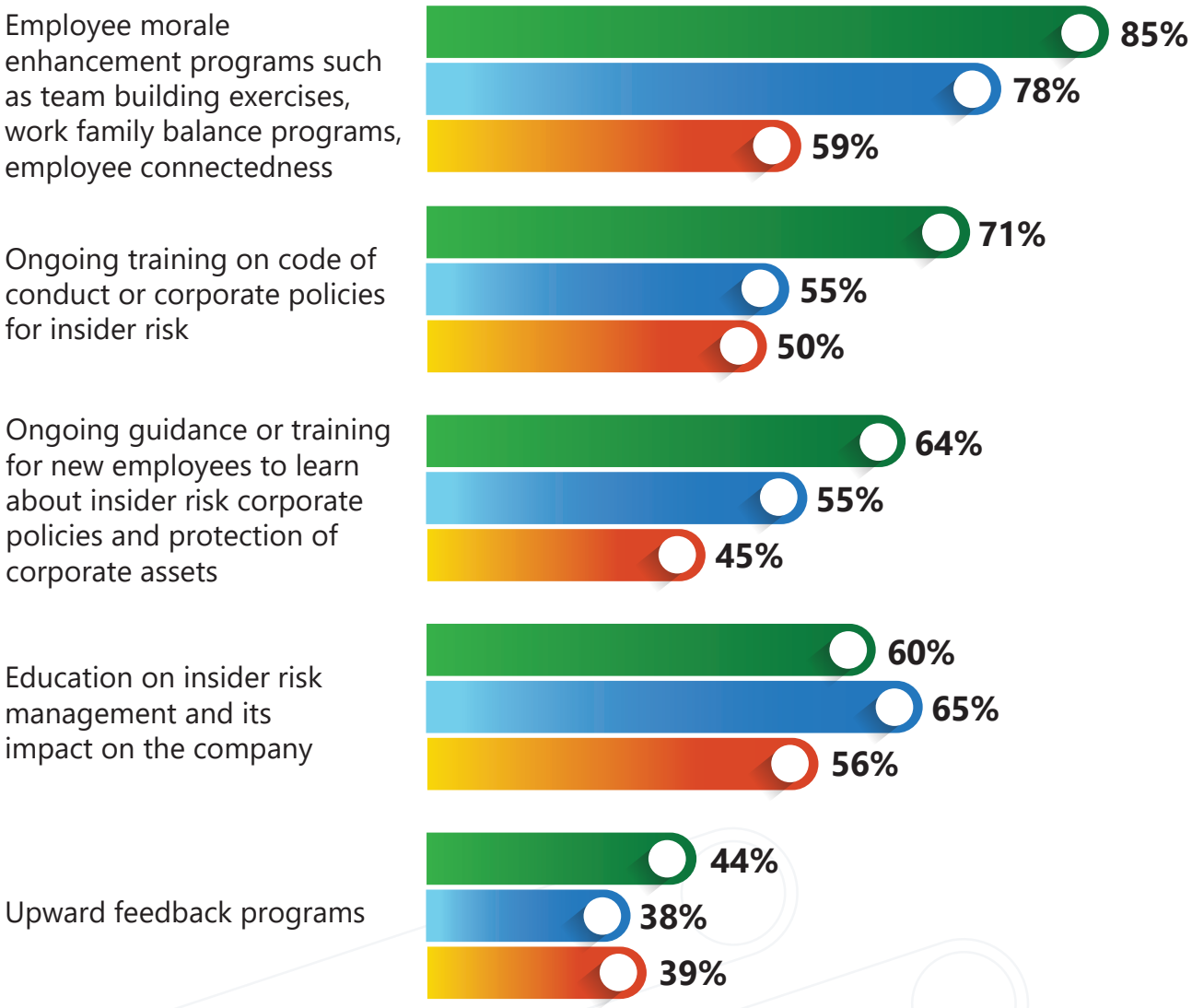


4 Use positive deterrents more often

Organizations that ranked high on our HIRMI utilized positive deterrents, such as employee morale events, more detailed onboarding, ongoing training, upward feedback, and work-life balance programs at a higher rate; they engage more preemptively with employees than evolving and fragmented firms. Positive deterrents help build and improve the employee-employer relationship, and foster trust, integrity, and employee buy-in.

They create a healthier work environment and directly address the risk at its source by targeting the potential problems that may cause an employee to engage in dangerous behavior.

Figure 14: Type of positive deterrents currently in use



Fragmented organizations are less likely to use positive deterrents and place more emphasis on technical discovery of events. ***Nearly 50% of fragmented companies have two or fewer positive deterrents currently in use.***

The level of agreement with statements about strong employer-employee relationships is another indicator of differentiation between holistic and fragmented programs.

More than 90% of holistic companies agree that stronger employer-employee relationships are critical to insider risk management.

"With a balance of positive and negative deterrence that is right for the organization, the insider risk program can become known as an advocate of employee well-being and a means for improving employee productivity, engagement, connection, and commitment for the benefit of both the employee and the organization overall."

From CMU-Cylab - Insider Risk Management Program Building: Summary of Insights from Practitioners

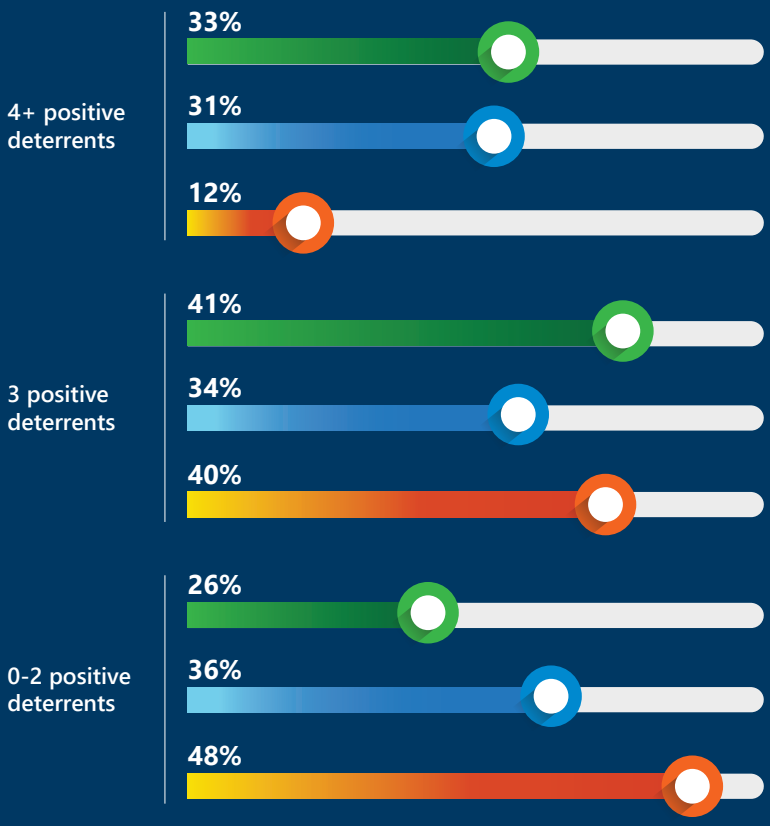


Figure 15: Number of positive deterrants in use

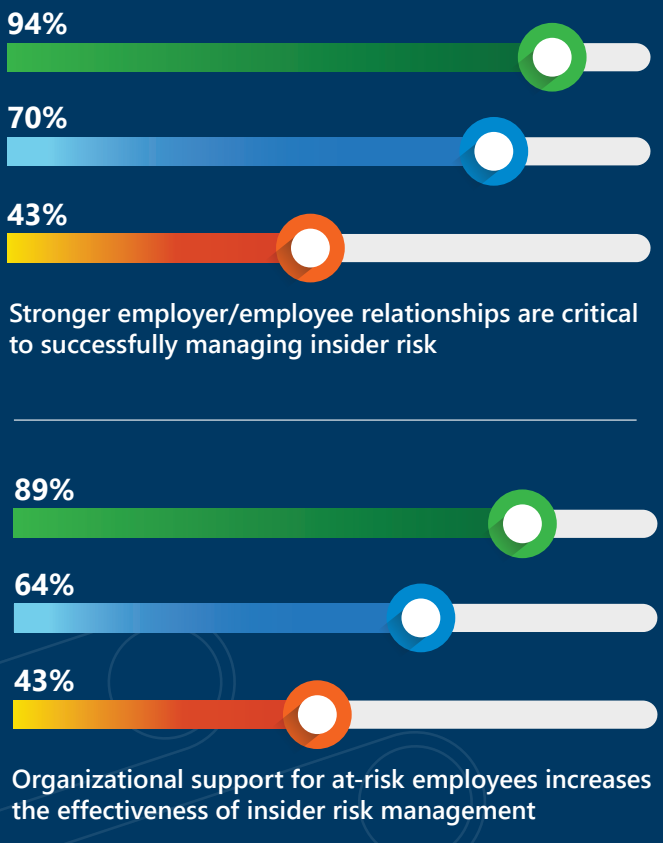


Figure 16: Level of agreement about employer-employee relationships

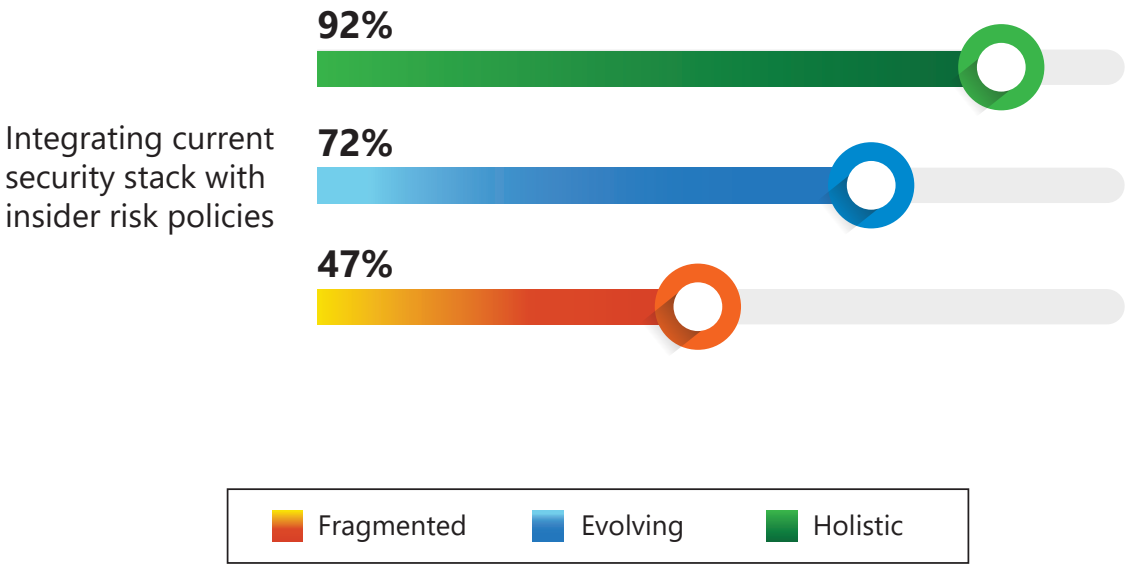
5 Integrate tool usage

Using the correct tools to help expedite detection and management of insider risk complexities is equally important to a successful program. Integrating tools into the existing security stack and creating visibility across the company are seen as vital to an effective program. Maintaining a balance of negative deterrents by leveraging risk-detection tools, such as Incident Threat Management (ITM), with an equally strong level of positive incentives is an effective approach used by holistic companies.

"Using the best tool for the job" is the IT mantra. But putting that into practice can be challenging. Holistic companies grasp the complexities of insider risk and place greater emphasis on an integrated tool stack that provides enterprise-wide visibility and up-to-date software.

Holistic companies display an increased use and integration of dedicated insider risk and IT security tools and policies that aid in detection and remediation.

Figure 17: Level of importance on success of insider risk due to integrated security stack



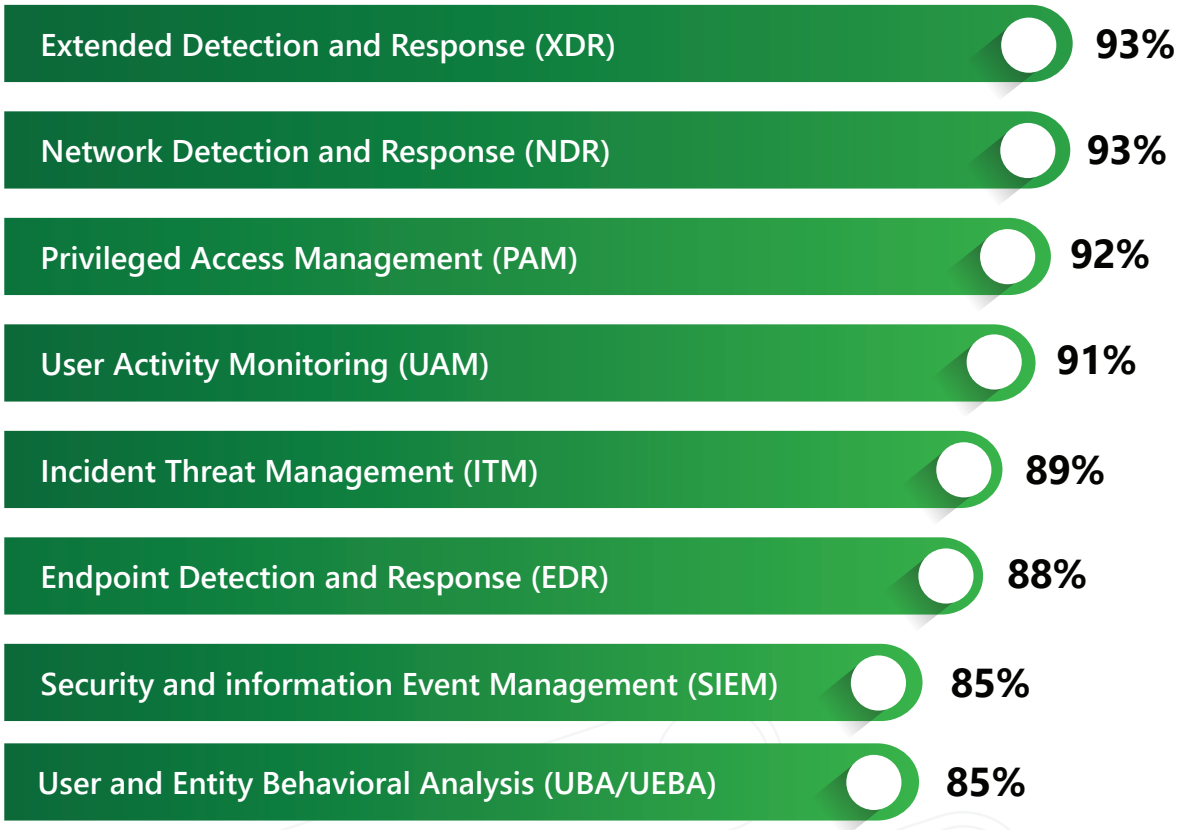
On average, the mean number of tools deemed critical to insider risk management is significantly higher among holistic organizations, providing a greater and more detailed picture of the insider risk playing field.

Figure 18a: Average number of critical tools used for insider risk detection

	Fragmented	Evolving	Holistic
Mean number of tools	2.8	5.0	7.0

Holistic organizations continue to enhance their capabilities across the company, widening their scope and improving opportunity for collaboration and success. Tools more often deemed critical by holistic companies are those also used for general IT security, such as, Extended Detection and Response (XDR), Network Detection and Response (NDR), Privileged Access Management (PAM), and User Activity Monitoring (UAM).

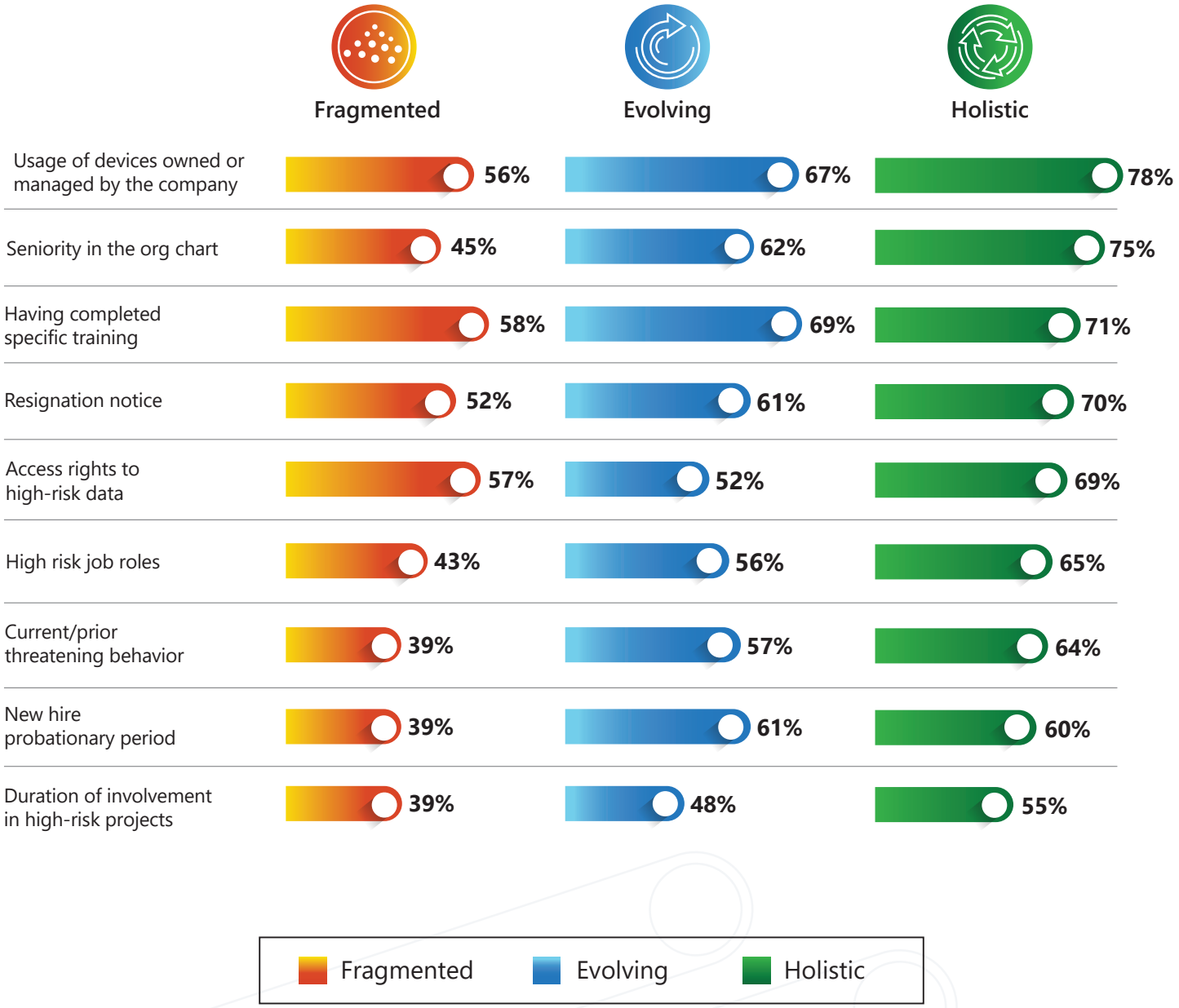
Figure 18b: Among holistic firms, tools deemed critical to insider risk management



This finding also ties into what we learned around scenarios that warrant more or less tool usage: the more scenarios in place, the more holistic your program.

Fragmented companies are less likely to have scenario-based triggering events around things such as probationary periods, seniority in organizational charts, and high-risk project involvement. Scenario-based triggering events can mean detecting when specific users take specific actions, like when an organizational leader accesses, downloads or exfiltrates particularly sensitive files, like confidential IP or revenue forecasts. Building policies around these triggering events can help define when and how investigations take place and may reduce the potential for system abuse by insider-risk investigators.

Figure 19: Scenarios leading to increased tool usage



"Negative deterrence is always going to be needed since some insiders will act out no matter how supportive the environment is due to other factors, but a combination of positive and negative deterrence can improve the effectiveness and efficiency of the insider threat defense over negative deterrence alone."

From CMU-Cylab - Insider Risk Management Program Building: Summary of Insights from Practitioners

How can being holistic help an organization?

The benefits of a holistic insider risk management program

Understanding how far along your organization is on our holistic index is essential. But knowing why you want to move up the index is equally as important. Our study points to some very useful impacts of a holistic approach.

Create a stronger company culture through a holistic approach

When organizations focus on strengthening relationships with employees, only positive things can come from it.

In the current world environment, creating strong bonds among coworkers, colleagues, and managers is an underrated element of successful organizations.

At the very least, if a company adopts a holistic approach to insider risk, it will incrementally improve the working environment of the organization, creating a better employee experience. At its best, a holistic program addresses the core of insider risk events—the employees—and educates, enlightens, empowers, and entrenches them in a company they care enough about to protect.

And in so doing, it should likely create more tangible benefits.

Potential reduction of events and faster detection

A tangible benefit from a holistic approach is the potential reduction of risk created by a more supportive environment. If the likely perpetrators of malicious insider events are disgruntled employees, a holistic approach helps reduce the potential numbers of disgruntled employees, thereby reducing the potential for any insider event in the first place.

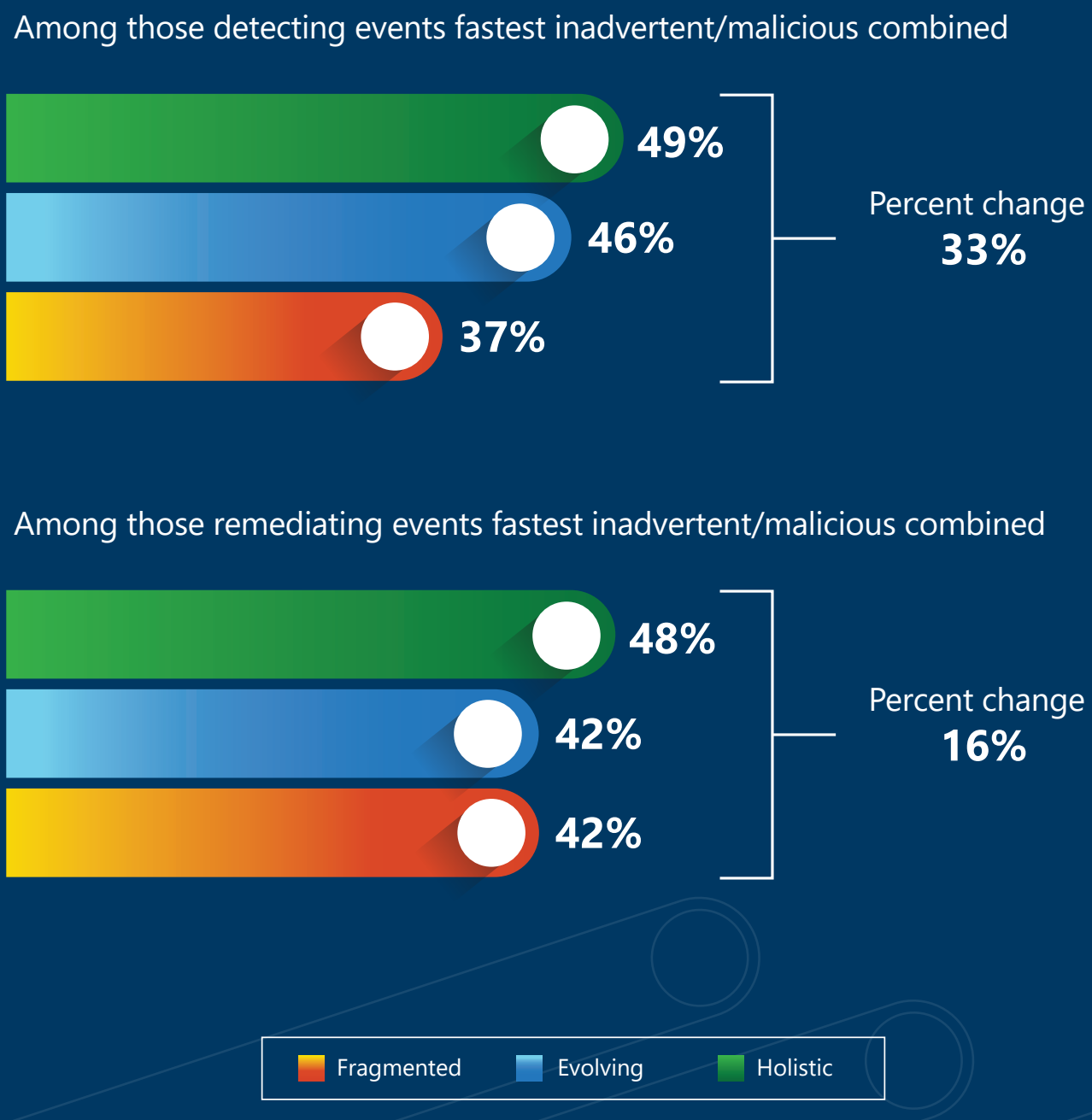
By engaging with employees at a higher level, creating programs that improve work-life balance, and fostering an environment that shows that the company cares, companies can help employees become more engaged with the training, take more heed of the warnings, and be more prepared to help observe and speak up about events, which would likely increase the speed of detection.

This could equate to thousands, if not millions, of dollars of potential cost savings as each potential event avoided reduces damage.

You might think that holistic companies who seek broad buy-in, protect privacy, and integrate their systems would achieve this only with a sacrifice in the speed of detection and remediation. But the data do not indicate that – in fact it shows the opposite.

Among the companies who were fastest at detecting insider-risk events, 49% were holistic and only 37% were fragmented. Among the companies who were fastest at remediating insider-risk events, 48% were holistic and 42% were fragmented. Thus, holistic companies in our sample were 33% more likely to have fast detection, and 16% more likely to have fast remediation, compared to fragmented companies.

Figure 20: Faster detection and remediation among holistic organizations

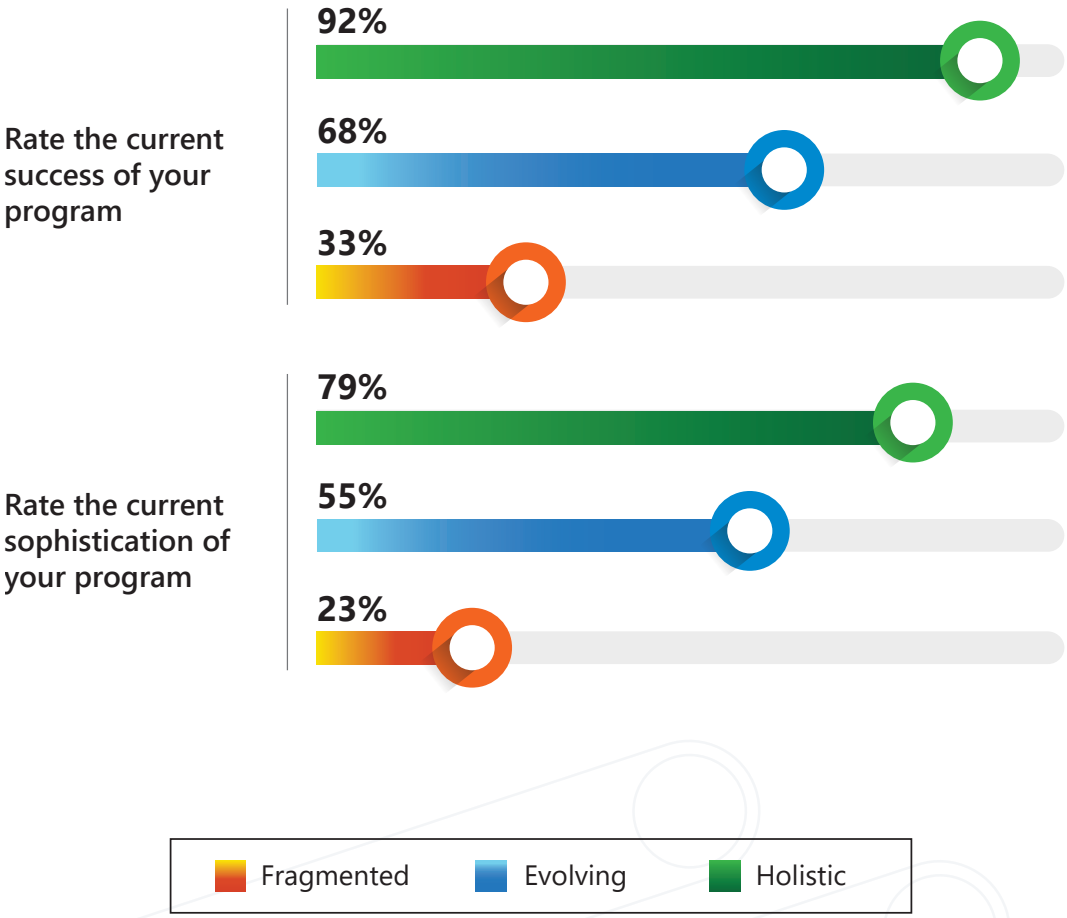


Perceived success increases among holistic companies

Defining success for an insider risk management program can vary by company and industry—detection speed, fewer false positives, and faster remediation certainly play a part. But there is more to a successful program beyond these hard numbers. Maintaining productivity, protecting employee privacy, and building trust can also be vital—and are all tied to a holistic approach.

An organization's perceived success and sophistication about its insider risk management program aligns with the HIRMI. Those using a more holistic approach feel more positive about their program and believe they are yielding better results.

Figure 21: Level of organizations' perceived insider risk program success and sophistication



Successful programs expect more events

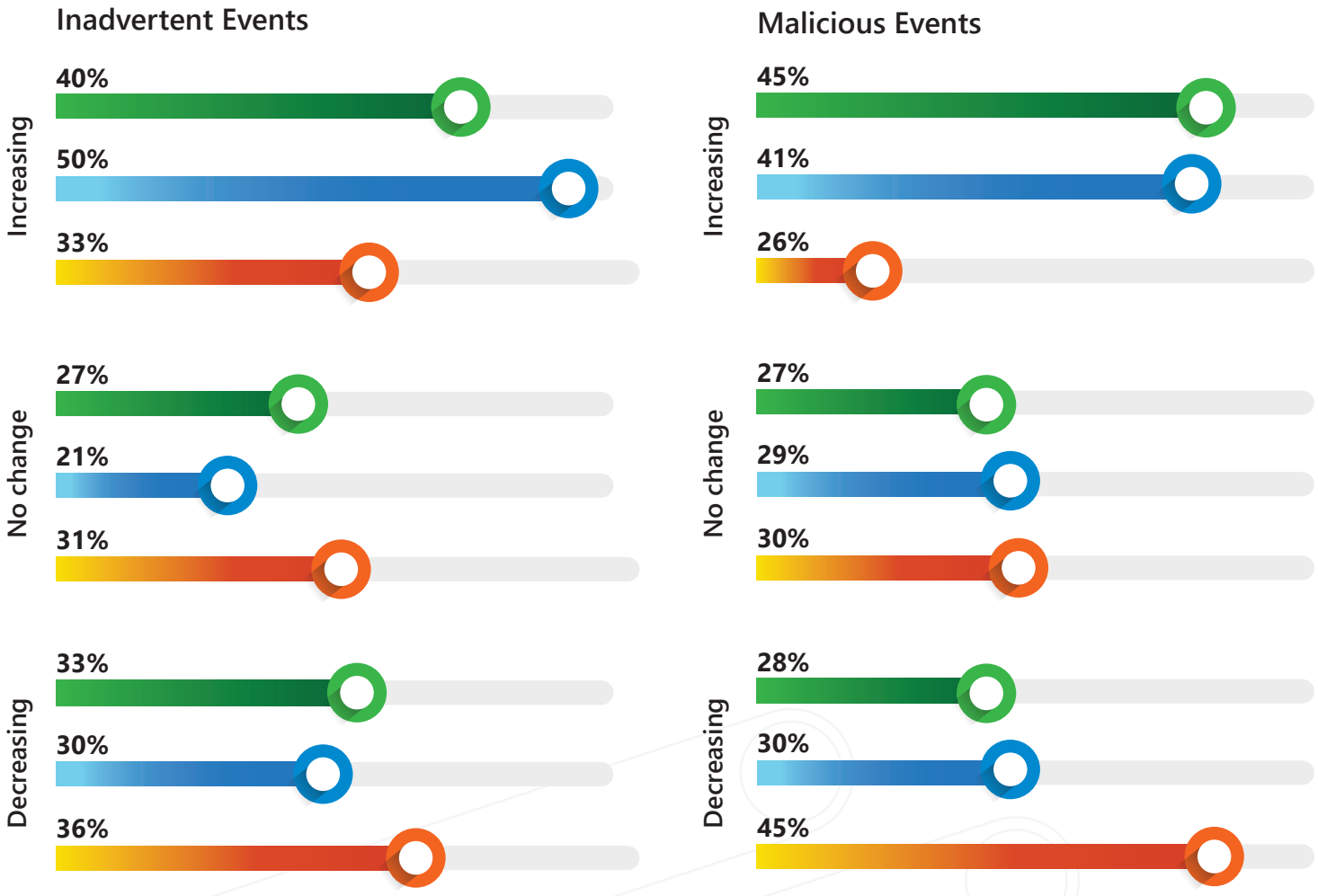
Holistic and evolving organizations are more likely to anticipate a rise in insider risk events in the coming year.

This seemingly counterintuitive finding can be interpreted as a holistic characteristic of these firms. They are more prepared for potential data security events and possibly more in tune with insider risk management. Although they might do everything they can to reduce their exposure to insider risk incidents, they also recognize how the world is changing and prepare for all possibilities.

Meanwhile, fragmented companies expect future insider risk events to decrease. Perhaps lack of data security awareness, an overconfidence in their program's ability to reduce events, or a reactive nature lead them to expect a more positive future.

Whatever the reason, the result is that fragmented firms might not be as prepared for the eventuality of insider risk incidents, leaving them in a vulnerable position that might take incrementally longer to detect and remediate.

Figure 22: Companies' expected change of future insider risk events



Where do we go from here?

In our research, we set out to discover how companies are handling insider risk management, and how they address the people, processes, training, and tools in their approach. We created the Holistic Insider Risk Management Index (HIRMI) and evaluated our findings.

The employee trust element surfaced again and again in our analysis. On one hand, employees are often identified as a source of risk stemming from lax access management related to user IDs and passwords. On the other hand, the research shows that employees—especially those with stronger relationships with employers—are seen by holistic organizations as important assets for mitigating insider risk.

How does a company intent on maximizing its insider risk program rectify the two seemingly opposing ideologies?

As we detailed in the paper, holistic firms work to ensure they increase their level of employee trust by fostering strong relationships. In doing so, employers build connections with employees who might end up protecting the company rather than attacking it.

As zero-trust strategies are becoming more prevalent, holistic organizations are better positioned to manage the complexities of insider risks and its impact on employees. A holistic firm's employee base will be better prepared to understand the reasoning behind data security and protection and more involved with the process. And, if employees care about the company, they are more likely to help protect it—again reinforcing our finding that trust is essential in all HIRMI elements. An employee-employer relationship rooted in trust can help build that first line of insider risk defense.

If your employees and departments buy in and are effectively educated, the impact on your organization can be profound. The key elements of a holistic insider risk management program harmonize to create a balanced approach built on trust and backed by a strong tool kit.

A holistic company can rely less on identifying and punishing, and more on using a positive organizational support that addresses the root causes of insider risk: employees who are negligent with data or deliberately taking steps to exfiltrate or leak data inappropriately.

Fragmented organizations just need to see the benefit of this different approach and can become holistic with some shift in company culture and attitude.

Organizations will continue to grow towards a zero trust-based model, and as they do, fostering employee trust and comprehensively addressing data protection should continue to be a focal point for success.

"We're not at a zero-trust model, but that's the goal."
- CISO, US Government

Best practices for building a holistic insider risk management program that fosters trust

1. Empower your people and make privacy a priority

To reduce risk and support the well-being of your employees, ensure they know they bring value to the organization and that they play an integral role in keeping critical data safe. Leverage open communications, put more emphasis on data security and protection education, and provide open channels for employees to voice concerns. Look for opportunities to add more privacy controls to underscore that their safety also matters.

---

2. Embrace collaboration across your leadership

Insider risk management programs often focus exclusively on implementing tools and technology without incorporating the necessary organizational, cultural, and employee support considerations. Technology plays an important role, but it's just one component of an effective program. Addressing insider risk requires a collaborative approach across business leaders, HR, legal, security, and more. It requires education, engagement, and buy-in enterprise-wide to create a comprehensive and effective approach.

---

3. Address insider risk from multiple lenses

Identifying insider risk incidents can be complex and might feel like trying to find a needle in a haystack. By taking a holistic, purpose-built approach to your data protection or insider risk management srategy and using integrated tooling that allows you to approach data protection from end to end, you can set the right policies for your sensitive data and gain a better eye toward insider risk reduction.

Conclusion

Managing insider risks is part of a comprehensive data protection strategy, and we advocate doing so in a thoughtful way that involves user privacy, cross-leadership collaboration, and a multi-faceted approach. Ensuring that you have the right people, processes, training, and tools in place can help your organization to better address the risks and challenges that you face as the data needs and landscape continue to evolve.

More about the study

Let's review our research methods and who we surveyed for this study.

Research methods

This study was commissioned by Microsoft and conducted by Concentrix Catalyst. We surveyed 300 United States-based security experts from companies of a variety of sizes and industries to understand what insider risk management challenges they're facing, the current state of their insider risk programs, and recommended elements of successful insider risk management.

Our fieldwork was conducted over a two-week period in July 2022. The researchers utilized quantitative surveys and qualitative interviews to capture and extrapolate data. Our final benchmark sample consisted of 300 separate respondents.

Organizations featured in the study included the following characteristics:

- 500 or more employees
- In commercial or public sector
- Based in the United States
- Respondents ranged from chief information security officers (CISO), security or compliance leads, and human resources, finance, or legal experts who are responsible for managing insider risk in the organization.

Composition:

- 300 United States-based security and compliance professionals
- 31% of survey respondents were categorized in "fragmented", 40% as "evolving" and 29% as "holistic"

Who we surveyed

INDUSTRY SECTORS

The three largest segments were computer or professional services, financial service organizations, and supply chain

COMPANY SIZE

Two-thirds of respondents came from companies with between 500 and 5,000 employees

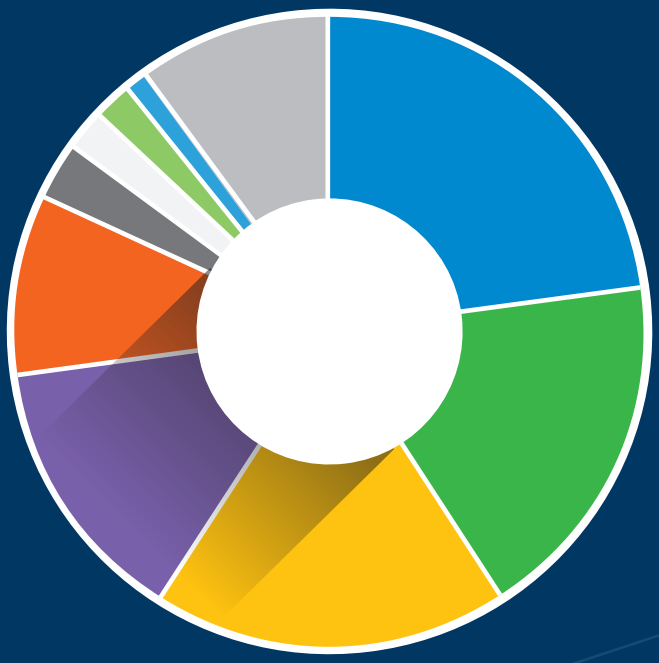
Meanwhile, 28% came from companies with between 5,000 and 50,000 employees, and 6% came from organizations with 50,000 or more employees.

POSITION LEVEL

More than 30% of respondents were at the C-level or VP/SVP level; almost 70% at Manager/Sr. Manager or Director/Sr. Director level

Approximately 31% of respondents were at the C-level or VP/SVP level, while 32% were at the Manager/Sr. Manager, and 37% were at the Director/Sr. Director level.

Figure A1: Primary industries



- **23%** Computer or Professional Services
- **18%** Financial Services (Banking, Financial Markets)
- **18%** Supply Chain (Electronics, Automotive, Aerospace & Defense, Chemicals & Petroleum, Other Manufacturing)
- **14%** Distribution (Retail, Consumer Goods, Wholesale)
- **9%** Health or Medical (Health, Healthcare, Medical Devices, Health Insurance, Pharmaceuticals)
- **3%** Energy & Utilities
- **2%** Telecom
- **2%** Public (Government)
- **1%** Media & Entertainment
- **10%** Other

Figure A2: Company size

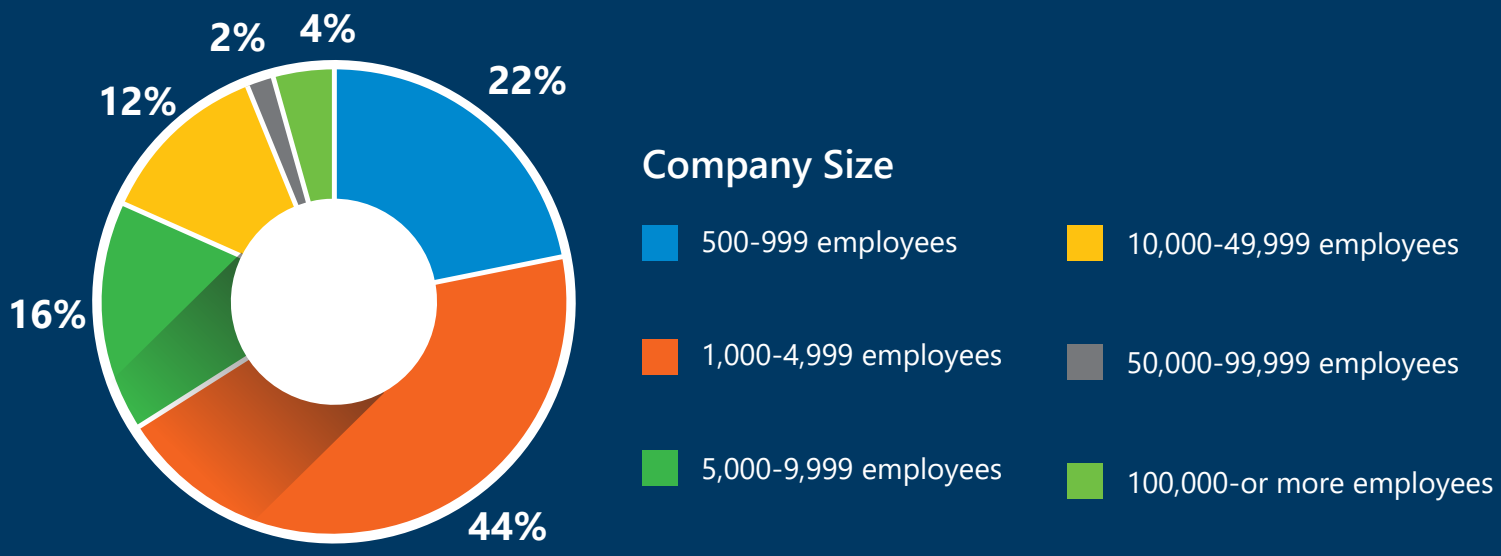
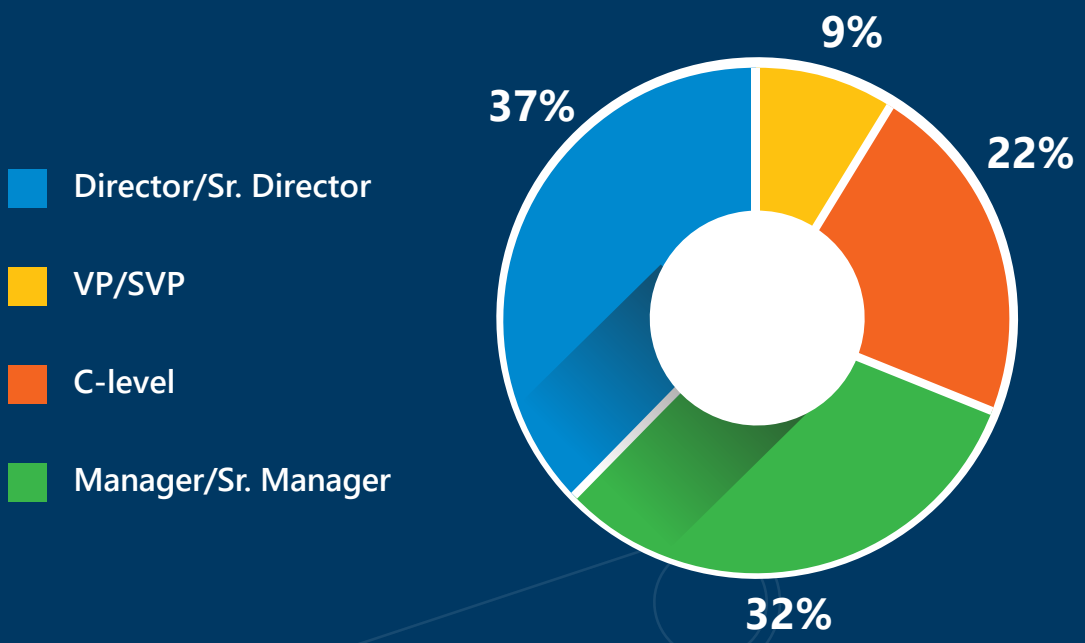


Figure A3: Position levels

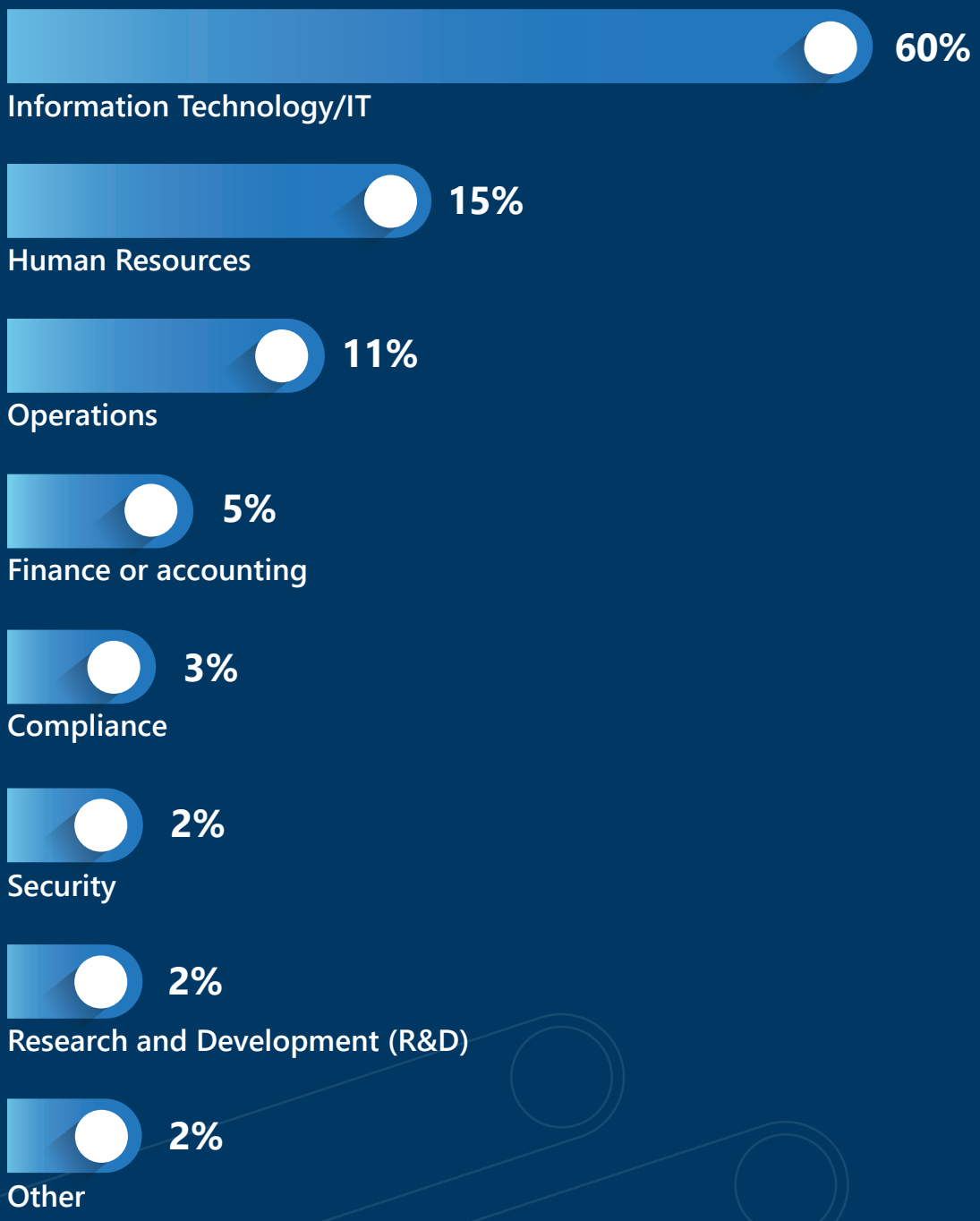


DEPARTMENTAL DISTRIBUTION

Nearly 60% of respondents worked in their organization's IT department

The majority of respondents worked in their organization's IT department. Meanwhile, 40% came from other departments, including human resources, operations, finance or accounting, compliance, security, and research and development.

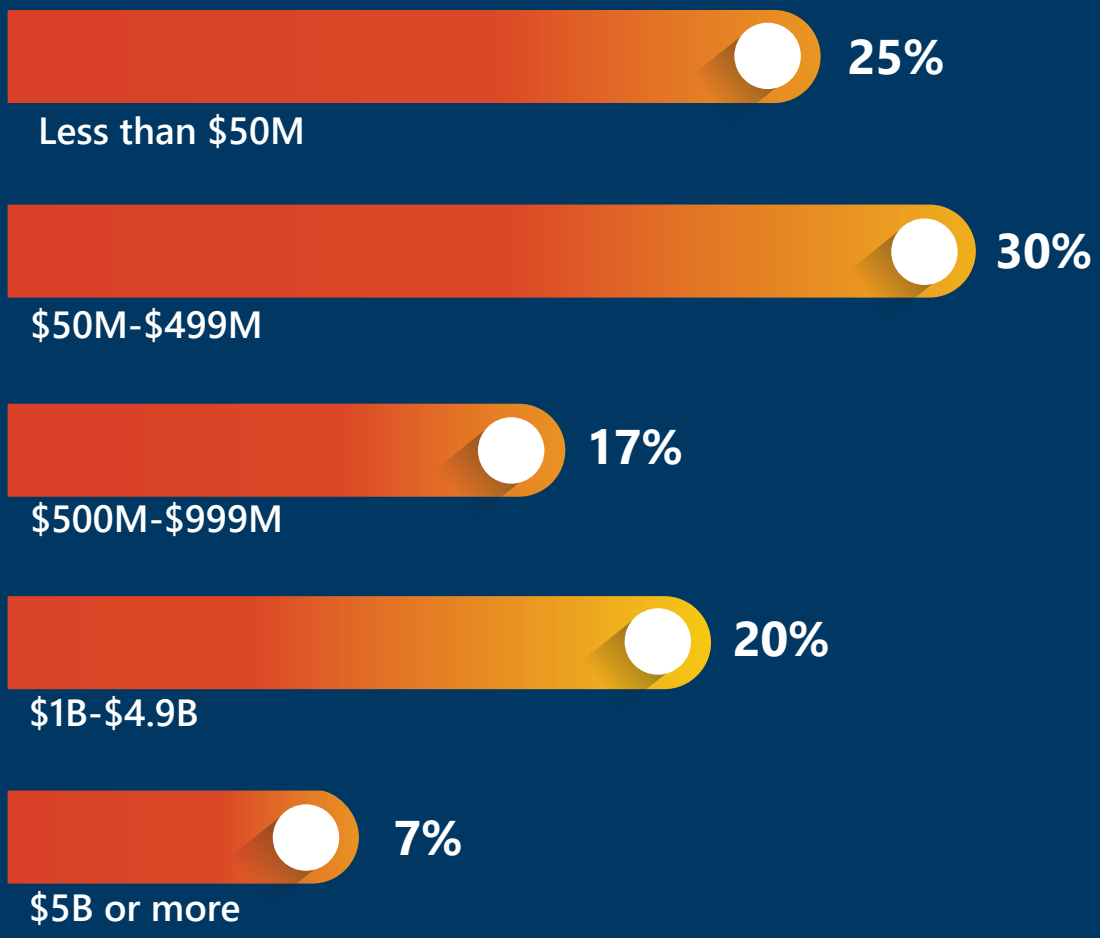
Figure A4: Departmental distribution



DISTRIBUTION OF REVENUE

Most respondent organizations (55%) reported revenue less than $500m
About a quarter (27%) of organizations had revenue over $1billion.

Figure A5: Organizational revenue



References

[1]Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025

[2]Microsoft Work Trend Index 2022. "Great Expectations: Making Hybrid Work Work"

[3]CyLab at Carnegie Mellon University. (2021) Insider Risk Management Program Building: Results from a Survey of Practitioners [white paper].

[4]U.S. Department of Justice (2021). Ph.D. Chemist Convicted of Conspiracy

[5]A. P. Moore, T. M. Cassidy, M. C. Theis, D. Bauer, D. M. Rousseau and S. B. Moore, "Balancing Organizational Incentives to Counter Insider Threat," 2018 IEEE Security and Privacy Workshops (SPW), 2018, pp. 237-246, doi: 10.1109/SPW.2018.00039.

[6]CyLab at Carnegie Mellon University. (2021) Insider Risk Management Program Building: Results from a Survey of Practitioners [white paper].