



# THE IMPACTS OF IDENTITY THEFT ON EMPLOYEES AND THEIR WORKPLACE



A PARTNERSHIP BETWEEN:



IDENTITY THEFT  
RESOURCE CENTER

[idtheftcenter.org](http://idtheftcenter.org) • 1-888-400-5530



## Identity Compromise Victimization

### Impacts On The Workplace

The workforce has evolved in recent years. With that, comes the evolution of technology as a day-to-day in how employees engage in the execution of their roles. Not to mention that today's employee has dramatically changed how they view their relationship with their employer. Benefits and perks have a substantial impact on how talent will determine where they want to work.

Is there a line between offering resources that provide security to the employee as a component of the benefit suite and the halo-effect for the employer? Cybersecurity is top of mind for most employers – from small business to enterprise – as well as their employees. On average, in 2019, an organization fell victim to [ransomware every 14 seconds](#). Marry that with a more than a one-in-four chance that a user will mistakenly click on a phishing email and infect a corporate network ([Osterman Research](#)), and there is substantial risk to every employer regardless of size.

### Organizations fall victim to ransomware every 14 seconds



One way that employers are solving this potential scenario is by offering their staff support for their personal identity compromises. The benefit can take many forms – from education on how to manage their personal risks and referrals to free resources, to paid services that run from voluntary benefits to fully employer-funded.

\*\*This report is intended as an educational tool to inform all stakeholders of the impacts of identity compromises on consumers and businesses.. The ITRC does not endorse, explicitly or implicitly, any product or service.



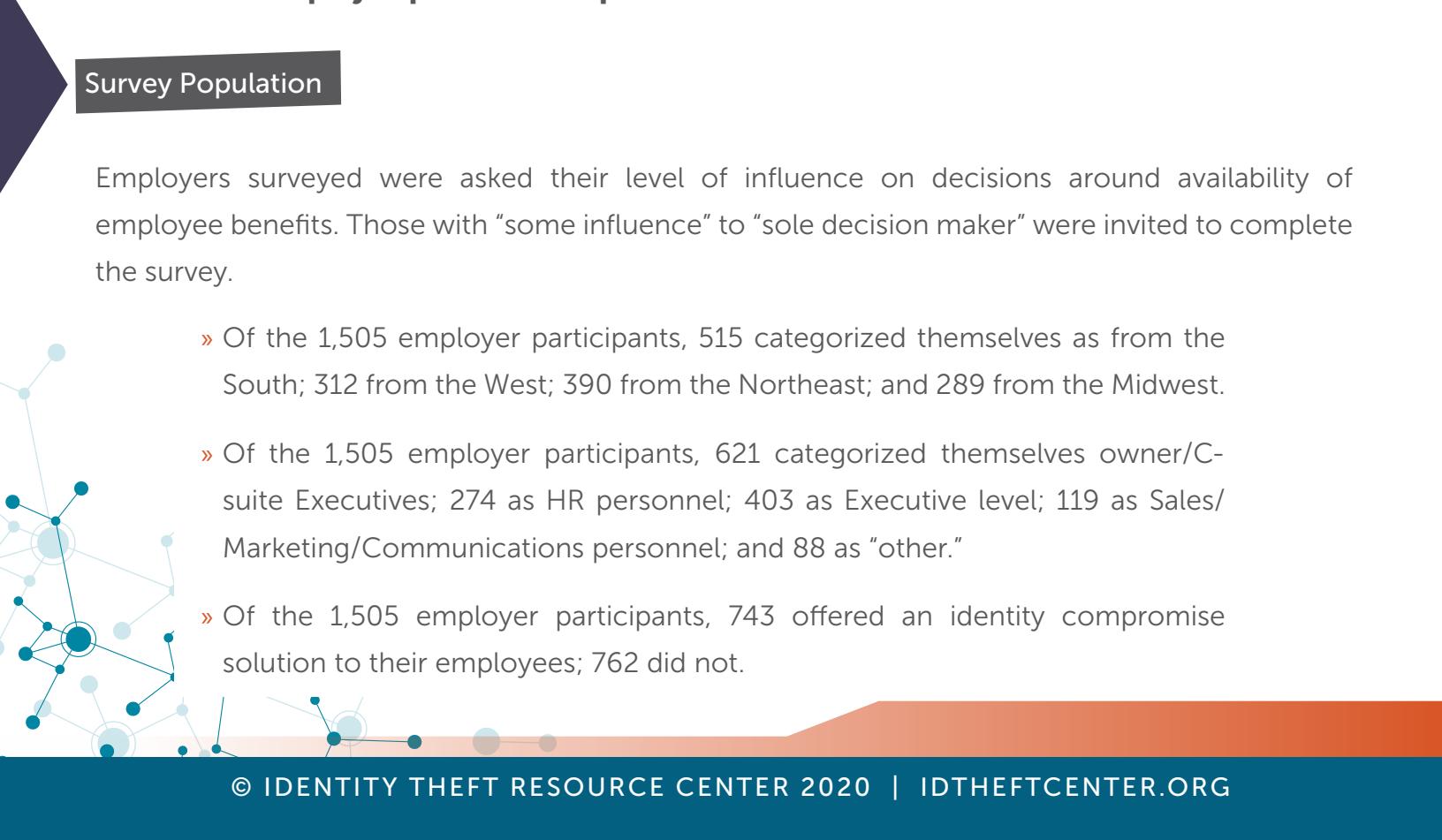
## Methodology

In an effort to gain some additional visibility into how employers and employees view identity compromise support as a benefit, the Identity Theft Resource Center® (ITRC) partnered with Aura™ Identity Guard® to survey both audiences on how they implement or utilize identity compromise solutions offered as an employment benefit. The ITRC and Aura Identity Guard polled a nationally representative sample of 1,505 employers (ranging from small- to enterprise-sized businesses) and 1,520 employees, who self-identified as victims of identity compromises, to gauge their perspectives on benefits that would support the resolution of their identity compromise.

**An “identity compromise solution” for the purposes of this study is defined as a resource made available to employees for their use in resolving their identity compromise.**

**This includes, but is not limited to:**

- » A referral to a free resource such as a non-profit or government agency
- » A voluntary benefit option available from their employer but paid for by the employee
- » An employer-paid benefit option



## Survey Population

Employers surveyed were asked their level of influence on decisions around availability of employee benefits. Those with “some influence” to “sole decision maker” were invited to complete the survey.

- » Of the 1,505 employer participants, 515 categorized themselves as from the South; 312 from the West; 390 from the Northeast; and 289 from the Midwest.
- » Of the 1,505 employer participants, 621 categorized themselves owner/C-suite Executives; 274 as HR personnel; 403 as Executive level; 119 as Sales/Marketing/Communications personnel; and 88 as “other.”
- » Of the 1,505 employer participants, 743 offered an identity compromise solution to their employees; 762 did not.



As part of the survey panel, employer participants were asked to provide their perspectives on if there was a value to their employees, as well their organization, to providing an identity compromise solution.

The 1,520 employee participants were asked to provide their perspectives on how valuable an identity compromise solution was as part of their employer-provided benefits suite. Those that identified as a victim of an identity compromise were invited to complete the survey.

- » Of the 1,520 employee participants, 491 categorized themselves as from the South; 340 from the West; 421 from the Northeast; and 268 from the Midwest.
- » Of the 1,520 employee participants, 798 identified as female and 722 as male
- » Of the 1,520 employee participants, 445 classified their income as between \$0-49,999; 374 as between \$50,000-79,999; 157 as between \$80,000-99,999; 544 as \$100,000 +
- » Of the 1,520 employee participants, 726 said that their employer did not offer an identity compromise solution in their benefit suite; 545 did offer it; and 249 were unsure of its availability.

As part of the survey panel, employee participants were asked to provide their perspectives on how having or not having access to an identity compromise solution impacted their case, as well as their perceived value of having access to a solution provided by their employer.

## Growing Impact On Employers

## And Employees



Improving cybersecurity is an organizational issue. It doesn't only sit with I.T. or security departments. Every employee is a potential vulnerability in the system. In a study conducted by Sapi Research, 79 percent of information security leaders said that employees are an effective first line of defense against cyberattacks ([SSD Technology Partners](#)). According to the [2018 BDO Cyber Governance Survey](#), there was a 350 percent increase in ransomware attacks, 250 percent increase in business email compromise scams and a 70 percent increase in spear-phishing attacks since its previous survey in 2017.



Couple the organizational impacts with how an individual employee could potentially be affected as a result of an identity compromise – from a decline in productivity to a spike in workplace apathy – and it's a recipe for disaster. The ITRC's [\*\*2019 Data Breach Report\*\*](#) reveals that 99.99 percent of the non-sensitive records exposed in 2019 were from business-related data breaches (705.1 million records). In 2019, the Federal Trade Commission (FTC) received more than 3.2 million reports of fraud with more reports of identity theft than any other category;

**99.99 percent of the non-sensitive records exposed in 2019 were from business-related data breaches  
(705.1 million records)**

the top issues noted in its Consumer Sentinel report were identity theft, imposter scams and telephone/mobile services fraud. The [\*\*International Foundation of Employee Benefit Plans\*\*](#) found that 96 percent of employers report that personal financial issues affect their employees' overall job performance. [\*\*Alight Solutions\*\*](#) found that 50 percent of workers want help getting identity compromise solutions. [\*\*Unum\*\*](#) reported that identity compromise solutions ranked in the top 10 (11 percent) of non-insurance related benefits for U.S. workers in 2019. One of the biggest

personal finance issues an employee can face is an identity compromise – from clearing out financial accounts to significant, systematic credit damage, it creates chaos and helplessness in its victims. There is an opportunity to support employees by providing access to an identity compromise solution that they are requesting. In this case, the evolution of how an employee looks at support from their employer has moved beyond the bread-and-butter insurance benefit.



In early results of its 2020 Aftermath™ survey, the ITRC found that 24.6 percent of victims who responded had issues with their employer as a result of their personal identity compromise and 27.3 percent reported challenges with their boss and/or coworkers. One victim reported his/her

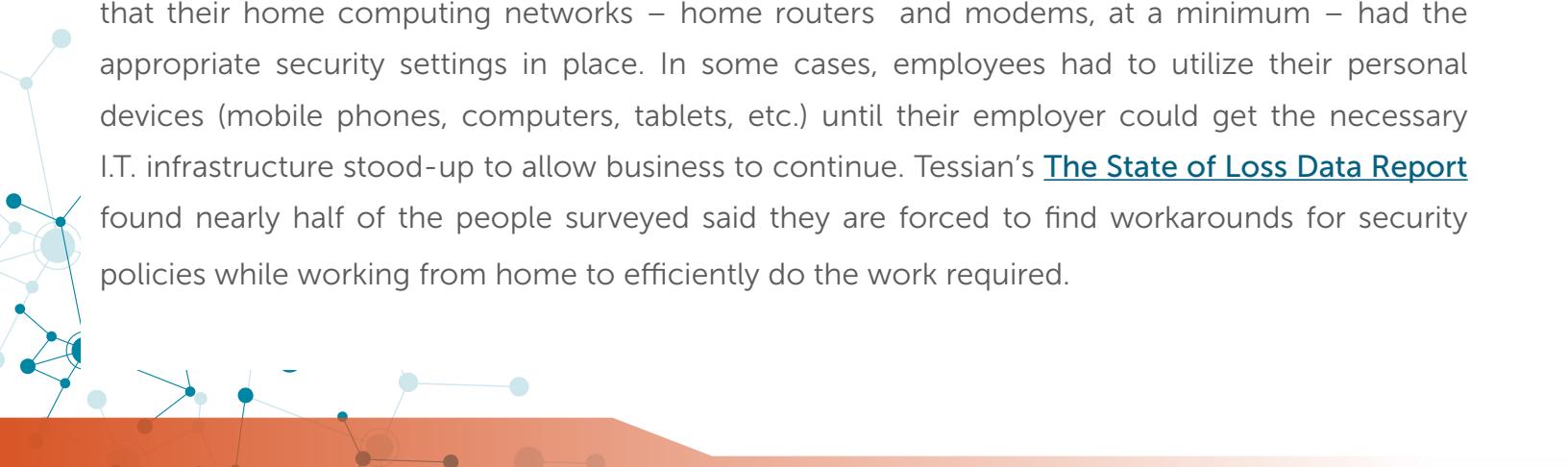


remediation process meant "time spent on lunch/breaks trying to get to the bottom of what was happening. A lot of calls were made during business hours, due to the time difference." [Pricewaterhouse Coopers](#) reported 33 percent of workers are distracted by personal financial issues; of those, 46 percent say they spend three or more hours each week dealing with related issues at work.

**“Time spent on lunch/breaks trying to get to the bottom of what was happening. A lot of calls were made during business hours, due to the time difference.” - Victim**

## How The Move To Remote/ Work-From-Home (WFH)

### As A Result Of The Covid-19 Pandemic Impacts Everyone



In the first half of 2020, employers and employees were thrown a curveball. The COVID-19 pandemic forced employers to rethink how to conduct business when federal and state governments, under the guidance of the Centers for Disease Control and Prevention, issued stay-at home orders for all nonessential businesses. Employers that wanted to ensure that they could continue to provide services, conduct business and avoid mass lay-offs quickly stood-up remote work/work-from-home policies to maintain business continuity. Many employees were thrust into a new and unfamiliar situation of ensuring that their home environment could sustain their work requirements. Employees were required to ensure that their home computing networks – home routers and modems, at a minimum – had the appropriate security settings in place. In some cases, employees had to utilize their personal devices (mobile phones, computers, tablets, etc.) until their employer could get the necessary I.T. infrastructure stood-up to allow business to continue. Tessian's [The State of Loss Data Report](#) found nearly half of the people surveyed said they are forced to find workarounds for security policies while working from home to efficiently do the work required.

## Nearly half of the people surveyed said they are forced to find workarounds for security policies while working from home to efficiently do the work required

From January 1 to July 9, 2020, the [Federal Trade Commission \(FTC\)](#) received 125,326 COVID-19-related reports, totaling \$80.99 million in total fraud loss, with \$274 as the median loss. Of those, 64,990 (51.9 percent) were indicated as fraud and 19,893 as identity theft (15.9 percent). Email as the method of contact accounted for 6,747 of the COVID-19 and stimulus fraud reports, with \$12.99 million in losses. In the first week of April 2020, the FTC began to see an upward trend in the number of identity theft reports, with the single highest day of reports being May 11, 2020 (489). July saw a leveling out of identity theft reports to an average of between 74 and 224 a day.

Cybersecurity experts report an [increase in exploits](#) like CEO spear-phishing, [phishing](#) and malware [posing as I.T. support](#), and more, as a result of the shift in a distributed workforce. While employees are accustomed to the support systems in-office, many new technology implementations resulting from the need to move to a remote workforce opened employees to malicious attacks to which they would otherwise not be exposed.



How does offering access to an identity compromise solution as part of a larger benefits program create positive outcomes for employers? It's more than just a conversation of cost. Identity compromise solutions can range from **free referral resources to employer-paid protection services** – and everything in between. While an employee is likely the biggest beneficiary of the outcomes from providing some aspect of an identity compromise solution, employers benefit from their workforce's increased awareness as a result.



Identity compromise solutions can range from free referral resources to employer-paid protection services

## KEY FINDING #1

---

# Employees Find Value In Having Access To An Identity Compromise Solution

It's not a surprise to most employers that benefits are a key tool in recruitment and retention. In a [2018 study](#), 78 percent of workers indicated they would likely remain with their employer because of the benefits it offers. [Accenture found](#) about two-thirds of workers would trade their work-related data for more customized compensation, benefits and rewards.

Employers that offered access to an identity compromise solution agreed (82.5 percent) that it provided a value to their staff. Companies offered a variety of ways to access identity compromise solutions with some offering multiple options:



**55.2%**

referral to a free resource like a non-profit or government agency



**55.6%**

an employer-funded benefit



**17.6%**

a voluntary benefit option for a paid service



Their employees agreed that the benefit held value. According to employee respondents that have access to one of the options for identity compromise solution:

- » They believed it would help resolve their identity compromise

Survey respondents said that they felt they were able to act on an identity compromise issue more quickly than if they hadn't had the benefit available (93.6 percent). Employees also indicated that they were able to resolve their identity compromise issue faster as the result of having access to their identity compromise benefit (91.02 percent).

- » 91 percent would encourage their work peers to take advantage of the benefit

In its [2019 report](#), Javelin Strategy identified 14.4 million Americans reported that they were a victim of identity theft. With nine out of 10 employees saying that they would recommend their coworkers take advantage of identity compromise solution, there isn't a better endorsement of its value to employees. [Nielsen cited](#) 92 percent of consumers trusted the suggestions of friends and family when it came to decisions – work is, by extension, part of this trusted network.

Not to be left out, ITRC and Aura Identity Guard also polled employees whose benefits package did not include an identity compromise solution.

When asked about if it were an available option, employees responded:

- » They believed it would be a beneficial option if it was offered (82.36 percent)



For those that didn't have it as part of their benefit offering, almost two-thirds indicated that they would use it if it were available to them for free – 61.33 percent would use a referral to a free resource like a non-profit or government agency; 67.28 percent would utilize an employer-funded service.

» **Half of employees would be willing to invest in identity compromise solutions as a voluntary benefit (50.15 percent)**



**67%**

**Would utilize an employer-funded service**

**61%**

**Would use a referral to a free resource like a non-profit or government agency**

[BenefitsPro](#) found that 62 percent of employees under 50 years of age wouldn't consider working for a company that didn't have voluntary benefits. Not only that, 19 percent are willing to pay more a month for services and tools that improve their financial situation (19 percent). Generation X employees – a little more than [one-third of the workforce](#) – would participate in financial programs if offered at work ([89 percent](#)).

What does that mean for employers? Choosing an identity compromise solution as a benefit option doesn't require the financial investment on behalf of the organization as some employers or benefits managers might think. Staff are willing to use free resources or invest in tools themselves if they are made available. Providing a free-to-use solution would significantly increase its adoption rate.



## KEY FINDING #2

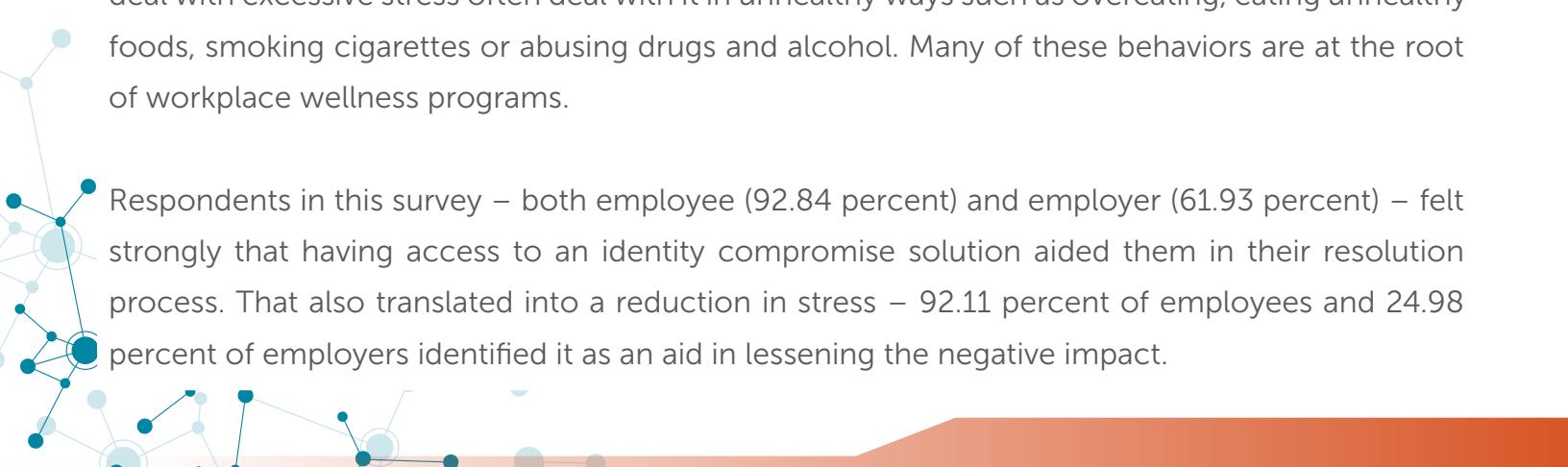
---

# Having Access To Identity Compromise Solutions Creates A Better Mindset For Those That Use It

In its 2018 Aftermath™ Study, the ITRC's victims had quite a bit to say about how their identity compromise impact their emotional and psychological well-being. Victims reported:

- » Getting into more arguments with family (36.4 percent) and friends (25.5 percent) as a result of their identity compromise
- » Engaging in more fights with family (15.2 percent) and friends (20.0 percent)
- » Feeling unable to trust family (45.5 percent) and friends (55.0 percent)
- » Not feeling supported in the process of resolving their identity by family (45.5 percent) or friends (65.0 percent)

These issues do not just stop at the office door. In many cases, these issues translate into work performance challenges. According to the [American Psychological Association](#), employees who deal with excessive stress often deal with it in unhealthy ways such as overeating, eating unhealthy foods, smoking cigarettes or abusing drugs and alcohol. Many of these behaviors are at the root of workplace wellness programs.



Respondents in this survey – both employee (92.84 percent) and employer (61.93 percent) – felt strongly that having access to an identity compromise solution aided them in their resolution process. That also translated into a reduction in stress – 92.11 percent of employees and 24.98 percent of employers identified it as an aid in lessening the negative impact.

Employees identified that access to an identity compromise solution also reduced the amount of time-off (paid and unpaid) required to manage the remediation of their issue (91.19 percent) a quarter of employers (25.15 percent) noticed a reduction in the amount of time-off need as a result of their employee's identity compromise. Employees also indicated that they felt like they had a better quality of life as a result of having an identity compromise solution available when they needed it (89.17 percent).



[Glassdoor](#) found that 87 percent of employees expected their employer to support them in balancing their life between work and personal commitments. Given that many find they are required to resolve their identity compromise during work hours, finding support from an employer or supervisor can be a challenge. Employers (61.6 percent) reported that offering an identity compromise solution to their staff allowed employees to stay more engaged during work hours, while employees agreed (88.62 percent). A majority of respondents in this survey (55.07 percent) said that they did feel supported by their supervisor/employer during their remediation process. Those feelings of goodwill translate into company loyalty.

## KEY FINDING #3

---

# There Are Key Benefits That Help Employers

When it comes to cyber-hygiene, the employee isn't the only beneficiary. In addition to a reduction in lost time – represented as time-off and time taken during work hours – mentioned in the previous section, organizations reap the rewards when an identity compromise solution is available as a benefit.

## More Cyber-Aware

According to [Small Business Trends](#), one-third of employees learn about minimizing cybersecurity risks from their family and friends (34 percent) and mainstream media (35 percent), with only 31 percent receiving cybersecurity training from their employer on an annual basis. In Shred-it's [State of the Industry](#) report, 47 percent of business leaders reported believing that human error by an employee led to a corporate data breach. Equipping frontline employees in their personal identity and cyber-hygiene equated to similar habits in the workplace. A vast majority (92.29 percent) of staff polled by ITRC/Aura Identity Guard said that as a result of their use of their identity compromise solution benefit, they were more aware of the security applied to their work accounts. Almost as many (90.45 percent), said that they were more invested in their company's security because of their awareness of their own cyber-hygiene as part of their benefit.



**Almost as many (90.45 percent), said that they were more invested in their company's security because of their awareness of their own cyber-hygiene as part of their benefit**

Employers also saw benefits from providing an identity compromise solution as a perk. FireEye's [Cyber Trendscape 2020 Report](#) highlights that just shy of half of Chief Information Officers (49 percent) believed their organization was ready to face a cyberattack or data breach. Small Business Trend cited 70 percent of its respondents rated their company as "excellent" or "good" when it came to their cyber-hygiene. Close to three-quarters (74.22 percent) of employers that offered an identity compromise solution felt that their organization was more aware of security best practices and could handle a cyberattack (70.36 percent). Some noticed that there was an improvement in organizational cyber-hygiene (24.98 percent).



**They also noticed that there was an improvement in organizational cyber-hygiene (24.98 percent)**

### Positive Employer Opinion

An employer's choice in the type of available benefits has a direct correlation to how it is perceived by its employees. Nearly 40 percent of employees say having a wide selection of benefits would make them feel more loyal to their employer ([MetLife](#)). In the same study from MetLife, 59 percent of employees say that health and wellness benefits are important for increasing loyalty to their employer and 53 percent say the same about financial planning programs.



Of the employees in the ITRC/Aura Identity Guard survey, 91.19 percent said that having access to an identity compromise solution gave them a positive opinion of their employer. Employers also acknowledged their awareness of their employees' appreciation of the benefit (41.13 percent).



**Employees in the ITRC/Aura™ Identity Guard® survey overwhelmingly (91.19 percent) said that having access to an identity compromise solution gave them a positive opinion of their employer**



# CONCLUSION

---

Selecting a catalog of benefits can feel like throwing darts at a moving target. It is hard to know what will be seen as a value for employees beyond the basic insurance aspects. Incorporating an identity compromise solution – whether that is a free referral to a non-profit organization like the ITRC or providing a service like Aura Identity Guard – gives the employee the support they need at a time of significant stress and creates a more cyber-aware workforce. As staff engage with their identity compromise solution, they gain more understanding and knowledge about how their behaviors and actions impact their personal identity hygiene that they can implement into their day-to-day work cyber-hygiene as well. The investment in creating those benefit offerings for the workforce will net the organization significant rewards of cyber-awareness in the long run.

*The ITRC may feature certain products or services offered by its partners, including Aura. We believe these products, as well as similar, generally available products may be appropriate for use by consumers or businesses to reduce the risk of fraud and/or identity theft. However, the ITRC does not directly or indirectly endorse or guarantee the performance or efficacy of any particular product, including the products referenced in this report.*

*To cite this report, please use the following: The Impacts of Identity Theft on Employees and Their Workplace case study, prepared by Identity Theft Resource Center (ITRC); Intersections Inc. dba Aura (2020) [idtheftcenter.org/aura](http://idtheftcenter.org/aura).*

*The ITRC encourages you to reference our research, analysis and information but requests you credit the Identity Theft Resource Center (ITRC) as the source and include a hyperlink to our [website](#). Altering the information or the ITRC's analysis is not permitted.*

*This research report was funded by Aura based on independent research conducted by the Identity Theft Resource Center.*



IDENTITY THEFT  
RESOURCE CENTER

[idtheftcenter.org](http://idtheftcenter.org) • 1-888-400-5530

3625 Ruffin Road #204  
San Diego, CA 92123

