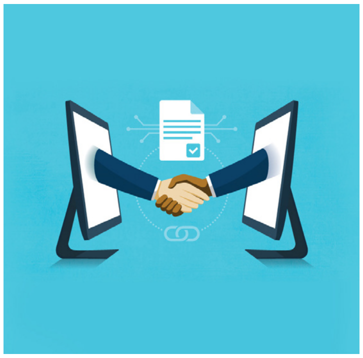
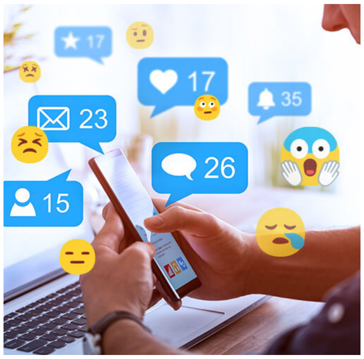
SECURITY MANAGEMENT

Powered by ASIS INTERNATIONAL
Advancing Security Worldwide®

Security's Role in Finding and Keeping a High-Functioning Workforce

This collection of articles from the security profession's premier publication examines security's key role in hiring new staff—and how to provide an environment where the staff can thrive.





SECURITY MANAGEMENT

Do Organizations Rely on Background Checks Too Much?

Do background checks provide a false sense of security? Lapses and loopholes in screening procedures have a history of coming back to haunt organizations.

By Louis R. Mizell, Jr., and Michael A. Gips, CPP

Background checks, preemployment screening, background investigations—by whatever name, it's the process of scouring criminal, academic, employment, and other records to verify that potential hires are who they say they are and have the background, education, and experience they claim.

A cornerstone of a sound security program, preemployment screening is used almost universally by employers; the Professional Background Screening Association indicates that 96.1 percent of employers perform some sort of preemployment background screening.

And most background checks in the United States run smoothly and effectively, in compliance with the U.S. federal Fair Credit Reporting Act, and with no complaint.

However, a worrying minority of cases show not only gaps in the system but also egregious examples of either abuse or poor oversight. It's also clear that background checks are not a failsafe or panacea, and should be only one key element of a personnel security program.

For more than 30 years, the authors have been analyzing cases in which lapses in background checks resulted in sometimes catastrophic loss or damage to people, businesses, assets, and the U.S. government. In more than 60,000 cases over the last 20 years alone, U.S. security, intelligence, military, and law enforcement personnel were charged with major felonies. But thousands of these individuals passed background investigations either by using someone else's name, ID, and Social Security number; or by lying about degrees, work experience, finances, arrest records, or citizenship status.

Pvassing a background investigation…is no guarantee that the employee is law-abiding, psychologically sound, or even who he or she claims to be.

Moreover, the data spotlights two harsh realities: passing a background investigation, even a properly conducted one, is no guarantee that the employee is law-abiding, psychologically sound, or even who he or she claims to be. Nor does it ensure that he or she won't break bad in the future. Over the last few decades, more than 120 cleared workers in almost every U.S. government department, intelligence agency, and military service stole U.S. secrets for foreign countries, betraying their country and destroying lives and livelihoods. The problem persists today.

CATEGORIZING LAPSES

The authors have identified 36 categories of issues that resulted in background checks that did not perform as they should have, including but not limited to investigators faking results, employers ignoring negative findings, employers relying on the honor system, and insiders deleting criminal records. We have placed these cases in four categories: the guile of the job candidate, the lack of specific requirements for what should be checked, the fault of the hiring organization, and the fault of the third-party screening provider. Many cases fall into more than one category or are difficult to place.

Guile. Criminals continually circumvent and outsmart the screening process. For example, in 2006 U.S. Border Patrol agent Oscar Antonio Ortiz, a Mexican citizen, was sentenced to prison for smuggling more than 100 illegal immigrants to the United States from Mexico, often transporting them in his own car. He had falsified a birth certificate to get the job. Before applying for the Border Patrol role, Ortiz had been arrested by his future colleagues for smuggling people across the border, but he had used a fake birth certificate to clear the background check.

A 2010 investigation uncovered that Nathaniel Brown changed his birth date and Social Security number by a single digit to get a custodial job at Ohio State University. The numbers he provided were not checked against official documentation, so his previous five-year prison term never came to light. He got the job, and after a poor performance review, Brown ended up killing his supervisor and wounding another man before killing himself.

Corrupt insiders contribute to the problem. The authors have recorded scores of cases in which staff at state departments of motor vehicles generated and sold fraudulent driver's licenses. Those schemes have placed pristine yet bogus IDs, which could later serve as breeder documents, into the hands of tens of thousands of individuals, including undocumented immigrants, criminals, and possibly even terrorists.

Scope of checks. In other incidents, background checks don't go far enough. Even though her sister was married to a member of the Cartel del Noreste, Jennifer Loya passed a background check for a lower level position for the U.S. Attorney's Office in San Antonio, Texas. Loya, eventually promoted to a paralegal, used her insider knowledge to tip off members of the cartel to imminent raids on drug caches by the U.S. Drug Enforcement Administration. She was arrested in May 2020 for obstruction of justice and conspiracy to possess and distribute methamphetamine.

According to the university, Roth began teaching there before the school's screening process was complete.

A background check of Yeshiva University lecturer Akiva Roth, who started working there in 2013, failed to turn up his 1997 guilty plea to four counts of lewdness against several boys in his role as a tutor. According to the university, Roth began teaching there before the school's screening process was complete.

Employer disregard. In still other cases, employers never conducted a search. Over a two-week period in late summer 2019, a pair of deliverymen in Palm Beach County, Florida, attacked women awaiting their purchases. One victim was beaten to death and set afire; the other was sexually assaulted. Both assailants had prior arrests, one from just the year before.

And in 2014, a Florida massage studio called Essentials was ordered to pay $47.4 million to a woman who sued after an employee touched her genitals during a session. Testimony at the trial revealed that the company had not conducted a background check on the culprit, who had been fired from three previous jobs.

Screener misfeasance. Screening companies themselves can contribute to the numbers of the wrongly cleared. Sometimes, criminal checks are requested but languish in a backlog. In January 2020, a high-ranking New York City education official was federally charged with using a computer to facilitate a child sex crime. Although he had been hired four years earlier, his background investigation had not yet been completed.

Screeners sometimes evade or abuse background checks for expediency and volume—exalting profit over probity. Industries with high turnover and high demand—including security guarding firms—often face pressure to fill roles quickly, sometimes without fully investigating candidates. U.S. Investigations Services (USIS), the company that cleared NSA leaker Edward Snowden and Navy Yard shooter Aaron Alexis, was sued in 2014 by the U.S. Department of Justice (DOJ) for notoriously clearing 665,000 background checks that had not been reviewed. From 2008 to 2018, the DOJ prosecuted 27 individuals for submitting fraudulent checks, by failing to interview sources or obtain key records, for example.

In 2017, Chicago officials were outraged after ridesharing service Lyft brought on a driver who had just served a prison term for aiding al Qaeda. Background screening conducted by the city of Chicago and by Uber previously disqualified the driver due to that very conviction, but Lyft missed it. In a statement to the press, Lyft wrote that the "independent background check provider should not have approved the driver, and that is unacceptable."

GOVERNMENT REFORM EFFORTS

"Government efforts to maintain a trusted workforce have, to date, fallen short," said the nonprofit Intelligence and National Security Alliance (INSA) on its Security Policy webpage. It continued: "Agencies' stovepiped approaches to security clearance investigations and adjudications leave the nation unprepared to counter adversaries who seek to harm our people, institutions, and infrastructure."

In light of the USIS scandal and other criticism, the U.S. federal government now requires a civilian government employee to review every background investigation file to disincentivize rushing through checks to bolster profits. In a certain percentage of cases, that person audits some of the checks by contacting sources that should have been interviewed. While no system is perfect, officials say results have improved.

Per an executive order signed by U.S. President Donald Trump in April 2019, the Office of Personnel Management relinquished all background investigation responsibility to the Department of Defense's Defense Counterintelligence and Security Agency. An official of the newly tasked agency testified that it had reduced the backlog of background investigations from a high of 725,000 open cases in April 2018 to 231,000 in January 2020.

While that's a promising start, INSA calls for further reforms, including passing legislation that would set time limits for clearance determinations and eliminate duplicative clearance investigations. The organization also calls for continuous evaluation, a process in which agencies steadily receive reports or alerts about staff arrests, convictions, license suspensions or revocations, and other relevant information from credit reporting agencies.

PRIVATE SECTOR EFFORTS

While asserting that background checks are more effective than they have ever been, experts acknowledge areas for improvement, some of which are underway.

Commenting on the 2010 Ohio State case, Illinois-based background screening expert and practitioner Nick Fishman calls it “one of the most egregious examples of how someone can work the system.” He says that the failure in that particular case stemmed from not requiring a valid form of ID and checking the job applicant’s application against it. “More and more companies are starting to do that extra check,” he adds. “But everyone should be doing that.”

When it comes to completed checks that do not catch troubling issues, Fishman explains that there is no set of standard checks for nonregulated industries. “The gold standard is to do a county check wherever they lived and using a Social Security trace to search all the names they have used,” he says. Then the screener would conduct a federal check and one of the national criminal database.

Although screeners can make suggestions, companies in unregulated industries can task screeners with whatever checks they want. “Generally, there aren’t best practices in background screening for unregulated industries,” says Fishman. And a limited scope of search is the most common reason that adverse information isn’t found when it could have been.

“If they’re not regulated, it’s all in the hands of the employer to determine how thorough the background check is," agrees Melissa Sorenson, executive director of the North Carolina-based Professional Background Screening Association. She adds, though, that there are common practices based on industry, job type, and job level.

For example, companies tend to check seven years of criminal records—certain states set that as a time limit and the original draft of the Fair Credit Reporting Act established that time period as well (though an amendment in 1998 did away with that limitation). Sorenson says that there is no movement afoot to set a standard for the scope of a background check. Doing so would be difficult, she says, because "there are so many moving parts." For example, reporting processes in the United States differ by type of crime—felony versus misdemeanor—as well as by federal, state, local, county, and city rules. And as a practical matter, what's accessible in one court might not be available in a neighboring jurisdiction.

Where Sorenson does see room for improvement is with respect to personal identifiers on public records. "We are seeing a trend among courts of slowly redacting personal information" for privacy reasons, she says. "It started with Social Security numbers…and now courts are regularly pulling pieces of data, only providing the month and year of birth." More detailed identifiers yield much better results.

SECURITY OFFICER SCREENING DEVELOPMENTS

The authors have identified more than 1,000 cases in which security officers passed background checks before committing crimes ranging from sabotage and espionage to rape and murder. Many should never have passed pre-employment screening. Underlying the issue is a patchwork state-by-state approach to regulating background screening for officers. Some states don't require screening at all.

"I'm sure there are unarmed security officers being hired in Mississippi now without background checks because there's no regulation, no legal requirement," says Eddie Sorrells, CPP, PCI, PSP, chief operating officer and general counsel at Alabama-based DSI Security Services.

Help may be on the way. Sorrells says that U.S. Senator Pat Toomey's (R-PA) introduction of S.3012, the Private Security Officer Screener Improvement Act of 2019, is a step in the right direction, although its fate in Congress remains uncertain. The National Association of Security Companies—whose member companies employ almost half a million security officers in the United States—explained in a press release that "the bill enables employers of security officers to obtain previously authorized FBI background checks on their officers and applicants from a DOJ designated entity when such FBI checks are not available through the state of employment."

Although screeners can make suggestions, companies in unregulated industries can task screeners with whatever checks they want.

While both the U.S. federal government and the private sector are improving some aspects of preemployment checks, glaring errors or shortcomings in the process still regularly produce tragic results. To some extent, the effectiveness of background checks is constrained by well-intentioned public policy positions, such as the desire to preserve citizens' privacy and enable ex-convicts to make a living after serving their time.

But the authors' data shows that breakdowns in the preemployment screening process continue to occur with disappointing regularity.

LOUIS R. MIZELL, JR., IS A FORMER INTELLIGENCE OPERATIVE AND ANALYST WITH THE U.S. DEPARTMENT OF STATE WHO HAS SERVED IN 105 COUNTRIES. HE HAS WRITTEN NINE BOOKS ON SECURITY AND TERRORISM, APPEARED ON PROGRAMS SUCH AS OPRAH AND THE TODAY SHOW, AND HAS BEEN QUOTED OR CITED IN MORE THAN 400 PUBLICATIONS. MICHAEL A. GIPS, CPP, IS THE PRINCIPAL AT GLOBAL INSIGHTS IN PROFESSIONAL SECURITY, A FIRM THAT PROVIDES SECURITY CONTENT, SECURITY STRATEGY, AND BUSINESS DEVELOPMENT. THE FORMER CHIEF GLOBAL KNOWLEDGE & LEARNING OFFICER AT ASIS INTERNATIONAL, HE HAS PUBLISHED MORE THAN 1,000 ARTICLES ON SECURITY. MIZELL AND GIPS HAVE DEVELOPED A KNOWLEDGE BASE OF MORE THAN 3 MILLION CRIME AND SECURITY INCIDENTS DIVIDED INTO 100 INTERRELATED SYSTEMS, INCLUDING BACKGROUND SCREENING.

SECURITY MANAGEMENT

The Background Check Dilemma in a Shrinking Labor Pool

In the competition for labor, employers may be prone to hire the first living, breathing person who applies. As tempting as it may sound, this hiring practice is fraught with danger.

By Steven Millwee, CPP

A Nassau County, Florida, jury found two trucking companies responsible for a crash that killed a college student and ordered them to pay $1 billion in damages.

University of North Florida student Connor Dzion, 18, was stopped on Interstate 95 on Labor Day weekend in 2017 due to a semi-truck crash ahead of him. While he waited for the interstate to clear, a tractor-trailer operator failed to stop and drove into a line of vehicles, including Dzion's. The college student was killed in the crash and 13 others were injured.

Dzion's parents filed suit against AJD Business Services, the semi-truck's company, and Kahkashan Carrier of Canada, the tractor-trailer's company, saying the crash that killed their son was the result of distracted driving and illegal trucking practices.

Curry Pajcic, a civil attorney with Pajcic & Pajcic, represented Dzion's parents in court. According to News4Jax, the semi-truck driver exceeded the number of hours he was legally allowed to be operating while in route from New York to Miami and was also driving without a commercial driver's license. Pajcic also said the driver was distracted by his cell phone when he crashed, which caused the traffic build-up on the interstate.

As Dzion sat in the traffic backup, Pajcic said, the tractor-trailer driver had his cruise control set at 70 mph and failed to stop, ultimately killing Dzion.

"Never hit his brakes until one second before impact," Pajcic said. "He failed to see stopped cars, a parking lot of stopped traffic with blinking lights, flashing lights, emergency vehicles."

The jury agreed with Dzion's parents and handed down a verdict of $100 million for pain and suffering and $900 million in punitive damages, citing AJD Business Services specifically for hiring a dangerous driver.

"The jury agreed the company did little to nothing toward safety and background checks before letting its driver behind the wheel," News4Jax reported. "Both companies remain in business but have not paid out the sums ordered."

NEGLIGENT HIRING

Under the doctrine of negligent hiring, an employer is liable for injury that its employees or agents inflict on third parties when the employer knew or should have known of the employee's potential risk to cause harm or if a reasonable investigation would have discovered the risk. Thus, background checks before placing employees in a position of trust or access to those where injury might arise are essential, according to the Society of Human Resource Management (SHRM).

THE CHALLENGE

One of the most significant challenges employers are facing today is the disappearing labor pool. Some companies are closing locations due to a lack of employees willing to return to work. Other employers have increased wages with little success to attract more employees.

A March 2021 survey by the National Federation of Independent Business found that 42 percent of owners had job openings they could not fill, a record high. Ninety-one percent of those hiring or trying to hire reported few or no applicants for the positions they were trying to fill, according to CNBC.

Employers may be prone to hire the first living, breathing person who applies.

PARTNERING WITH HR

Employers may be prone to hire the first living, breathing person who applies. As tempting as it may sound, this hiring practice is fraught with danger. Beyond claims of negligent hiring, experienced HR professionals and managers realize that hiring quality personnel through careful screening protocols pays dividends in the long run.

Security can leverage its expertise and partner with HR to review background screening protocols and selection of background screening providers. HR is looking for internal stakeholders as a natural fit to utilize their investigative skills in pre-employment screening. Although a $1 billion verdict certainly gets one's attention, preventing loss of life and promoting a positive working environment through careful background screening should be our common goal.

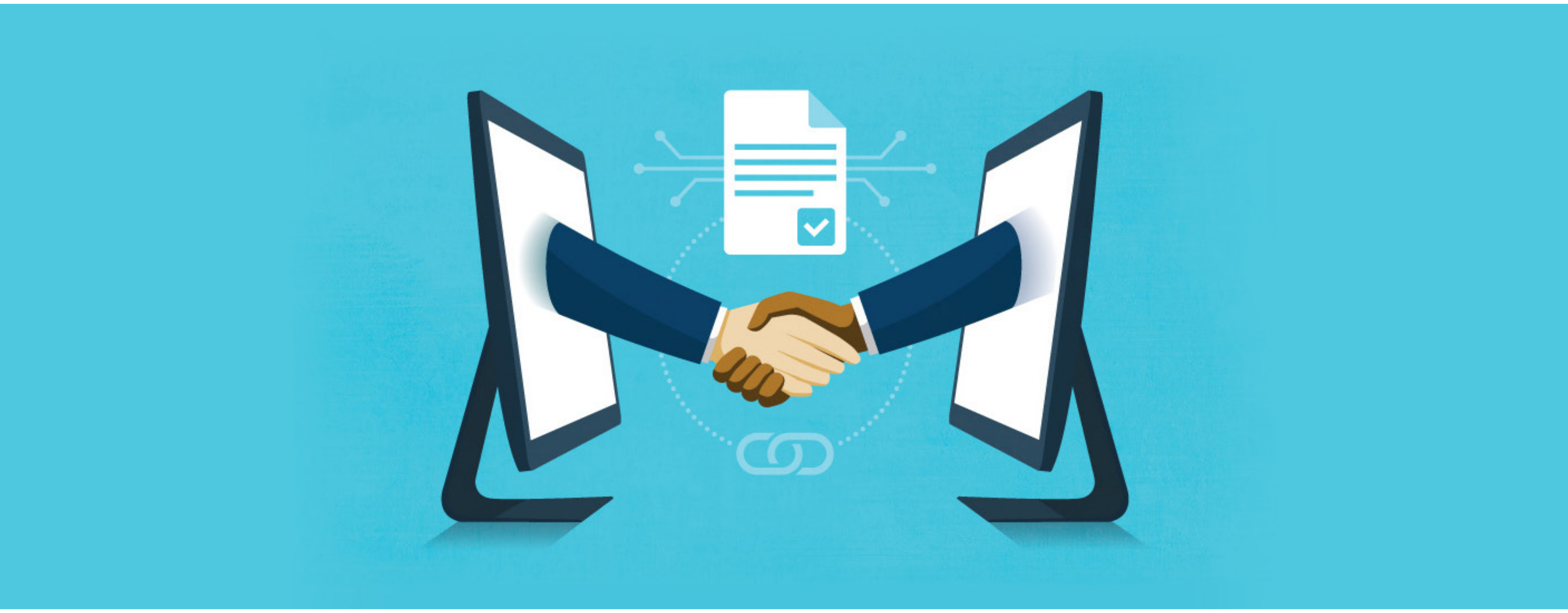
STEVEN C. MILLWEE, CPP, IS THE CEO AND FOUNDER OF SECURTEST, INC., A GLOBAL BACKGROUND SCREENING FIRM HEADQUARTERED IN PANAMA CITY, FLORIDA. MILLWEE IS A NOTED EXPERT WITNESS ON NEGLIGENT HIRING, SECURITY, AND WORKPLACE VIOLENCE FOR MORE THAN 42 YEARS AND IS A PAST PRESIDENT OF ASIS INTERNATIONAL.

SECURITY MANAGEMENT

Onboarding Beyond Zoom

Millions of people are transitioning to new roles. As onboarding shifts virtual, CSOs have an opportunity to leverage a new normal of online meetings to begin adding value faster and more effectively.

By Erik Antons, CPP, PSP



2020 was a kick to the head. According to COVID 19 and The World at Work, published by the International Labour Organization (ILO), "In 2020, 8.8 percent of global working hours were lost relative to the fourth quarter of 2019, equivalent to 255 million full-time jobs."

I was one of those statistics. In June 2020, my corporate security department was shuttered, and I lost my job as the CSO. The subsequent job search and onboarding process was largely virtual, which presented new challenges and opportunities for an incoming CSO.

Although the ILO report projects that robust recoveries will occur throughout many industries in the second half of 2021, there remains great uncertainty, and in the interim, millions will be in transition. This means greater numbers of people are now competing for fewer jobs and many will be asked to do even more with less—not only joining new departments within organizations, but in some instances tasked with leading teams with fewer resources.

According to a May 2021 article in the Harvard Business Review, 70 percent of firms are opting for a hybrid approach where some employees work from home, others work in the office, and some split their working hours between home and the office.

The meaning derived from a visual, however, is as much about the context in which we see it as it is about the image itself.

Whatever model is adopted, one thing seems consistent: At least part of the workforce will be working remotely in the coming years, and that comes with unique challenges from interviews to onboarding and onward.

FINDING THE BREAK-EVEN POINT

During a casual chat with an HR leader at a former company, I once asked what the expectation timeline was for new hires. The HR leader said that, in general, the first year for most is a time of learning about the company culture and processes. Expectations during this time were very low. This is a net deficit for the company, in which the employee is taking more value than they're producing.

According to the HR leader, a new employee at this company was expected to provide as much value as they are taking at around the six-month benchmark. This is known as the break-even point, and it varies depending upon the expectations of the organization, the job, and industry.

Regardless, this timeframe can be accelerated with effective onboarding strategies, enabling the employee to add value to the organization much faster and securing one's status within it, according to an article from the MIT Sloan Management Review, "Getting New Hires Up to Speed Quickly."

THE ESSENTIAL ONBOARDING INTERVIEW QUESTION

Before landing the job, there's usually a question for leaders—particularly toward the end of the interview process—that is something akin to: "How would you spend your first few months on the job?" It's a brilliant query that can provide insight into a candidate's prior research on the company and the job, as well as his or her ability to think tactically, operationally, strategically, and perhaps even politically. It can provide insight into the candidate's leadership style, prior experience with transitions, and perhaps most importantly, whether a candidate would fit into the company's culture.

Answering this question sufficiently is critical, so it's important to prepare for it by first researching the company and the role. This should have started before the initial screening interview and developed during the interview process.

If you have a corporate security background, you should have fundamental investigative skills, so approach every interview as a case. What do you know about the incumbent or previous person in this position? Are there any burning platforms—emergencies requiring immediate attention? Why does the organization need to fill this role?

What do current and past employees say about the company's culture? What did the organization's last 10-K report say about the company's financial status?

It's also a great time for self-reflection. What has worked well for you in the past and what hasn't during similar transitions? Is there anything you wish you had done differently if you had the opportunity? Not only might you be starting a new job, but others might be leaving—how could this affect your onboarding experience? Most importantly, what do you think you can do to establish credibility and trust as quickly as possible?

Perhaps an appropriate preamble response to this interview question could be something like: "What we're talking about is onboarding, and research has shown that an effective onboarding program can get someone to the break-even point—where one is providing as much value as they're taking much faster with an effective onboarding program. Overall, it's about establishing credibility and trust as quickly as possible, and in order to do that, based on my research into this role and the company, I think I would _____."

It might be easiest to lay out goals at the 30-, 60-, and 90-day timeframes. Be specific enough to connote the research you conducted and insight you developed, but general enough to project your leadership style and personality. Keeping current pandemic travel and work restrictions in mind, be realistic with your timeframes. Also, your responses may be less about what you know and more about whether you would be a good fit.

At the close of the interview, ask the interviewer if your onboarding response seemed reasonable. Though the interviewer may not provide confirmation, you may gain some insight as to whether or not you answered adequately, thereby further preparing you for a similar question during the next round of interviews.

YOUR FIRST 90 DAYS

Congratulations, you got the job! Pre-pandemic, the first 30 days would normally be a time of intensive one-on-one meetings, site visits, and training sessions to learn about the business, identify and engage with stakeholders, align expectations, and adapt to the culture.

Now, however, this is likely to take place virtually, which can seem daunting, given that offices may be closed and travel is severely restricted. The good news: most companies have adjusted their expectations to allow for more time to hit the break-even point and since travel is so limited, more people should be available for virtual meetings.

The four key elements of the framework— culture, organizational values, politics, and environment— all significantly influence how meaning is derived from an image.

As a result of the interview process, you should have identified some reasonable goals for your first 30-, 60-, and 90-day timeframes, and your new company may also have provided general expectations.

Perhaps for the first 30 days, the goal is to simply understand your company's fundamental administrative systems, establish rapport with your team, supervisor, and department, and identify some quick wins and any burning platforms. Maybe by day 60, you should have met with all critical stakeholders, completed visits to core production sites (if permitted), diagnosed your situation, and identified resources needed to complete some quick wins.

By day 90, perhaps you could be tackling some quick wins or generating a deliverable to demonstrate your expertise and motivation, contributing to the enterprise.

During the first 45 days at my current company, I had 39 onboarding calls with everyone from administrative assistants to regional presidents. This was very different from the past, when I likely would have spent the majority of my time in the field to gain an understanding of the current state of the organization—but like many other things, this was changed by the COVID-19 pandemic.

This time, upon being hired, I started scheduling 30-minute calls or virtual meet-and-greets with as many people as possible. From the interview process, you should have identified stakeholders who will be critical for your success. Ask your supervisor to help you identify others he or she thinks would be helpful.

First, speak with your direct reports and then work your way up the chain of command within departments, such as legal, HR, risk management, sales, procurement, logistics, and any others critical to your department. Include administrative assistants—they are the gatekeepers to senior management and can be among your most trusted sources of insight. Also, try to identify the "company historians"—those who have been around for a long time and know what works, what doesn't, and can provide insight as to why. Consider including external stakeholders such as suppliers, customers, analysts, and distributors.

Administrative assistants are the gatekeepers to senior management and can be among your most trusted sources of insight.

With each interview, you will learn more and become more polished, applying what you learned in each successive call. Save calls with senior leaders for last, by which time you should be highly educated about the company, will have your talking points polished, and can avoid potential landmine discussions that could cause friction.

Your calls should be short and keep the first few minutes very informal, which—as in the conduct of an investigative interview—is important for establishing rapport. Resist the urge to talk too much, especially about yourself. Remember, this is an opportunity for you to learn about them, the company, and the culture, as well as a chance to leave a favorable impression of yourself. After essential rapport-building, you will have only about 20 minutes, but if you ask the right questions, you can mine quite a bit of information.

In his book The First 90 Days: Proven Strategies for Getting Up to Speed Faster and Smarter, author Michael Watkins suggests several questions to ask during onboarding calls. Among them, I suggest the following three, at minimum:

- What are the biggest challenges your department is facing (or is likely to face) in the near future?
- What are the most promising unexploited opportunities for growth?
- If you were me, what would you focus on for the next 90-120 days?

You're essentially asking the same question in three different ways, or triangulating, as is often taught in interviewing courses. Reactions to these questions will vary, but responses should be relatively consistent.

Frontline workers may be frank and eager to provide specific, tactical answers; after all, they are often closest to the action. Responses from senior management may be additionally insightful and strategic given their vantage point. Regardless, responses to these questions will help identify the situation into which you walked.

Keep your calls short and be efficient with your time.

Something to remember, especially in a virtual format, is that Zoom fatigue and COVID burnout, although relatively new terms, are all too real. Don't be boring!

As a result of these calls, you should be identifying any immediate needs, areas for improvement, and some quick wins needed to establish trust so critical for your success. By documenting these responses, you now have data to back your plans. Further, you will, hopefully, leave the interviewers with a favorable impression of you—you made the most of your time with them and expressed a genuine interest in the company and your position within it, thereby increasing your credibility and influence.

The comments and views expressed in this article are the author's alone and may not reflect those of his employer.

ERIK ANTONS, CPP, PSP, IS THE CHIEF SECURITY OFFICER OF WHIRLPOOL CORPORATION WHERE HE IS CHARGED WITH SAFEGUARDING 81,000 EMPLOYEES AND NUMEROUS ASSETS ACROSS MORE THAN 170 COUNTRIES. HE WAS PREVIOUSLY CHIEF SECURITY OFFICER OF HYATT HOTELS CORPORATION, MANAGER OF INTERNATIONAL SECURITY WITH SEMPRA ENERGY, AND A SPECIAL AGENT WITH THE DIPLOMATIC SECURITY SERVICE AT THE U.S. DEPARTMENT OF STATE.

SECURITY MANAGEMENT

Turning Bad Apples Good: Using Soft Skills for Threat Assessment

In cases where an individual's values clash with the organization's, negative emotions—sadness, frustration, anger—can result in inappropriate behaviors and choices.

By Paul Wood, CPP

Actions, thoughts, and emotions do not exist in isolation. The way they interact will influence your perception of the world around you. Alongside attempting to meet your basic and psychological needs, as emphasized by Abraham Maslow in his influential paper "A Theory of Human Motivation," our behaviors are influenced by the way we experience feelings of confidence in our personal and professional activities or how we feel valued and respected by our friends, families, teammates, and wider social structures.

When individuals' values align with the organization's, this expression can be positive. In cases where those values clash, negative emotions—sadness, frustration, anger—

can result in inappropriate behaviors and choices. This can be detrimental in the workplace and requires employees to be empowered with the knowledge of potential insider threats and options available to mitigate them which can include behavioral analytics systems, data loss prevention tools, ongoing vetting, and internal employee monitoring processes.

In fostering a multidisciplinary approach to countering insider threats—involving insider protection teams, intelligence and investigations, legal, and human resources—an educational campaign can provide employees with confidence that they can operate openly and quickly to help mitigate risk.

Security professionals can also take proportionate and cost-effective action to managing insider threats by proactively managing disgruntled employees.

REFLECTION REQUIRED

All employees should strive to provide a strong example of appropriate behavior that both develops and underpins an effective business and security culture. If an employee's behavior breaches those expectations security leaders may benefit from taking the time to observe the incident and ask some reflective questions.

- Who am I looking at, and are they behaving differently?
- What did I expect them to do, and how was their action different?
- Where did this take place, and do I think the location or circumstances may have influenced the observed behaviors?
- When did this take place, and do I think it may have influenced the observed behaviors?
- How could they have performed differently? What can

they learn from this experience? How can I manage or approach this?
- Why did they behave that way, and was it appropriate?

This proactive approach to managing risks to teams, business processes, intellectual property, and confidential information takes a different stance to traditional security—it assumes that people have good intent. Such threats may be averted through emotional, rather than security intelligence. Employees who identify a change in the behavior of others can act quickly to engage with the individual in question to investigate concerns, detect threats, offer support, or escalate concerns.

This proactive approach takes a different stance to traditional security—it assumes that people have good intent.

For example, asking why someone may be acting in a way that is unexpected and considering whether something in his or her personal life may have influenced his or her behavioral choices. This can provide leaders with an opportunity to use soft skills to demonstrate care to employees and increase team unity and loyalty, which in itself can positively benefit security posture. In addition, posing reflective questions to employees to encourage them to consider their choices' impacts can provide growth opportunities, which will help develop them as both individual practitioners and team members. Such reflective practice can be performed during team performance reviews, after service incidents, and potentially after engagements between individuals that were observed as being potentially inappropriate.

Such a caring approach may in fact be the support the employee in question needs to get back on track to being the high performer you originally invited to join the team.

There are a range of training resources available—in addition to Daniel Goleman's essential book, Emotional Intelligence—to develop communication skills and an awareness of emotional intelligence. Behavioral change takes time, however, and managers seeking to adjust security culture may need to be patient with employees and colleagues.

Managers seeking to adjust security culture may need to be patient with employees and colleagues.

Managers seeking to adjust security culture may need to be patient with employees and colleagues.

If security leaders are advising asset custodians and managers about how they can approach this shift, they might consider three conditions that are commonly accepted as prerequisites for malicious activity: opportunity, rationalization, and incentive. Leaders should also consider the ways that one—or all of them—can be reduced during a period of behavioral change to protect the business and to give the employee the best chance of success.

Opportunity can be reduced through the design and implementation of asset protection systems. The personal motivations of employees can be influenced through a range of employee loyalty rewards and schemes, which can be financial or focused on positive reinforcement of appropriate behaviours.

BUILDING DEEPER CONNECTIONS FOR THREAT ASSESSMENT

Taking the time to develop a deeper understanding about colleagues and employees can play an important role in the development of a holistic risk management system. It will help security leaders assess situations and judge them against expected behaviors. A phased approach can be adopted.

Take the time to develop an understanding and awareness of team members. Getting to know employees plays a crucial role in motivating them to deliver their best work, and it can help managers understand their needs and the organization's expectations. This is crucial information for determining whether team members are happy with their jobs, whether they feel ignored or left out, and if anything may be going on in their personal lives which could influence behavior.

Identify security threats and risks. It is imperative that assets are identified and classified according to sensitivity and value. Through a business impact analysis, security leaders can determine what the effects would be if assets are damaged or fall into the wrong hands. Managers and employees should become familiar with the security threats to their organization and team, and leaders should provide clear information about the behavior that is expected of employees.

Determine appropriate security behaviors. Appropriate security behaviors should be determined in line with your organizational security policies, and all team members should be briefed on the expectations. Team performance can then be assessed against the security policies and the identified security behaviours to identify vulnerabilities and mistakes and respond or adjust accordingly.

Determine existing levels of security knowledge and awareness. It is important to determine what a team knows and what they do not know about security policies and procedures. The identification of skills and knowledge gaps will enable you to design appropriate training programs

Encourage your team to care. Ensure that security conversations form part of your regular team meetings so that all employees have an opportunity to inform others of their concerns or questions. Team members should be encouraged to take the time to check in with each other. Along with holding regular calls or meetings to provide project updates, dedicate time to caring for each other by asking questions and taking an interest in what motivates team members, what their interests are, and what challenges them. This can help team members and managers identify when a behavioral change has taken place, giving colleagues and managers an opportunity to divert the person from becoming a potentially harmful disgruntled employee.

Act quickly. Security breaches can happen anywhere and at any time. Reporting, record keeping, and response systems must be in place to ensure that risks are tracked and mitigated as quickly as possible. ▨

PAUL WOOD, CPP, IS THE MANAGING DIRECTOR OF EMERGING RISKS GLOBAL. HE HAS EXTENSIVE EXPERIENCE LEADING GLOBAL INTELLIGENCE AND SECURITY SERVICES IN GOVERNMENT AND CORPORATE ENVIRONMENTS. ALONGSIDE BEING AN ASIS CERTIFIED PROTECTION PROFESSIONAL (CPP), WOOD IS A UK CHARTERED SECURITY PROFESSIONAL, FELLOW OF THE INSTITUTE OF SECURITY, PRINCIPAL MEMBER OF THE REGISTER OF SECURITY ENGINEERS AND SPECIALISTS, AND SERVES ON THE ASIS CSO TECHNICAL COMMITTEE AND THE BSI INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION COMMITTEE.

SECURITY MANAGEMENT

Employee Activism as a Risk Management Opportunity

The combination of increased activism and elevated divisiveness presents a heightened threat for conflict entering the workplace, particularly for corporations whose employees are returning to the office after working remotely.

By Michael Center and Diana M. Concannon

Preparing for the probability that employees, or those with whom they interact, will offend one another is a logical modern risk management strategy.

Hyper-polarization, fueled by misinformation and the mainstreaming of fringe beliefs, has significantly increased the likelihood that individuals in the workplace will disagree on emotionally charged issues—particularly if the content has been politicized.

Political activism has hit record highs. In the United States alone, Civis Analytics estimates that 23 million residents engaged in some form of protest during 2020, the largest numbers in recorded history. Sources for political information also changed during the past couple of years. Increasing numbers of individuals now rely on social media platforms for their political news, despite widespread distrust of social media platforms as sources of truth, and heightened awareness of the ways in which social media algorithms amplify polarization, found researchers for a study in *Proceedings of the National Academy of Science*.

As more people become locked inside their own echo chambers, political perspectives often deteriorate into partisanship, and conflict can arise when engaging with those of differing views.

For example, a 2020 Pew Research Survey found that nine in 10 Americans said there is strong conflict between those of different political parties.

The combination of increased activism and elevated divisiveness presents a heightened threat for conflict entering the workplace, particularly for corporations whose employees are returning to the office after working remotely.

These threats can take several forms.

As many corporations have learned, the workplace itself can become the object of employee activism if the workforce believes that the organization can—and should—do more about particular causes.

In the aftermath of a mass shooting at one of its stores, Walmart employees conducted walk-outs to protest the chain's gun sales. Google employees also staged walkouts to protest lack of executive action on claims of gender discrimination and sexual harassment. And when cryptocurrency firm Coinbase attempted to stifle workplace activism by censoring dialogue not related to the corporate mission, 60 employees reportedly quit the company causing the directive to go viral.

Reputational damage and loss of talent are two prominent threats posed by employee activism. But the strategy to mitigate them should not overshadow the opportunity to fortify an organizational culture of safety, engaging in the challenge of accepting diversity of opinion without generating animosity.

Security professionals are positioned to play a key role in proactively assisting executives to manage employee activism in a manner that minimizes conflict and disruption.

An effective strategy relies on human intelligence—listening and gleaning information on the current priorities and perspectives of the workforce. True human intelligence requires emotional intelligence, relationships, and trust, which necessitates a security force that is well-integrated with, rather than siloed from, the workforce.

This information becomes the basis for strategic decision making. Different tactics are suggested by various findings. If there is general cohesion of thought among those within the company environment, there is an opportunity to strengthen workforce loyalty by subtle or overt forms of support for shared causes. These acts—from simple (mentioning the issue in a corporate newsletter) to significant (financial investment in an organization that supports a key issue)—can strengthen staff loyalty, a trait that supports workplace safety. Loyal employees are more likely to report unsafe conditions, comply with safety protocols, and resist unsafe or criminal activities.

If great disparity exists among employees, enlisting experts to help facilitate difficult dialogues models tolerance for non-disruptive engagement. Should the corporation be the target of advocacy—such as when Goya Foods was subject to a boycott for its CEO's political comments or the backlash against Dr. Seuss Enterprises for deciding against reprinting a few of its titles due to racist depictions—identifying the informal advocate leaders in the workforce and initiating solution-focused conversations between these individuals and corporate leadership—even if what is being sought is not achievable—can assist in building trust, which is foundational for conflict resolution.

Clear communication of behavioral expectations for employees who experience significant disagreement is also an important part of a risk management strategy. Such expectations—which should be congruent with corporate culture—can span a continuum from pausing engagement in non-work-related discussions that cause disruption until a formal forum can be scheduled to the expectation that differences of opinion will be tolerated and respectful listening or disengagement are required.

Explicitly communicating these expectations in a statement that reinforces the corporation's general commitment to diversity and intolerance for discrimination and harassment helps employees navigate a potentially divisive environment before it devolves into a more serious, conflicted one.

Decisions regarding workplace tolerance of visual displays—such as activist email signature blocks, Zoom backgrounds, and office décor—should also be explicit to preempt misunderstandings. Likewise, the workforce should be educated about general policies related to making public statements or participating in acts of civil unrest while wearing corporate insignia.

As with any risk management strategy, the tactics adopted as part of activism risk management need to reflect the culture and goals of the larger organization. And, as many corporations have learned in the past several years, when it comes to activism, the corporate culture may also need to expand to align with a more socially and politically engaged workforce.

AN EXERCISE IN APPLYING CONTEXTUAL INTELLIGENCE

By using the COPE (Culture, Organizational values, Politics, and Environment) framework to assess security challenges and potential flashpoints, leaders can help their institutions navigate complex situations and mitigate reputational risks. For a glimpse of this framework in practice, see the hypothetical case study below.

Entity. A small, rural liberal arts college in the United States with 700 students, 150 core and adjunct faculty, and 80 staff.

Challenge. A university that prides itself on diversity of thought and freedom of expression—and is legally bound to respect civil liberties and academic freedom—is experiencing increased incidences of campus disruption and conflict as students, staff, and faculty vocalize opposing views both on and off campus. The incidents are compromising the quality of campus life. Some in the campus community have reported that they are fearful that the conflict will become violent.

COPE FRAMEWORK ANALYSIS

Culture. Although a comparatively liberal work environment (flexible work schedules, relaxed dress code), the college's employees and students represent diverse populations along every demographic. There is a shared belief in the value of education, although opinions vary as to whether education should principally advance societal or individual goals.

Organizational Values. The college has a strong and well-articulated commitment to diversity and inclusive excellence. Its core mission also includes supporting its graduates to apply the education they gain to resolve complex, real-world situations.

Politics. Prior to the amplified social and political polarization of the past several years, the college frequently confronted divisions among students, faculty, and staff with different worldviews. The use of words such as “safe spaces” and “triggers” are common when individuals are confronted with encounters or material that range from the uncomfortable to the legally unacceptable.

There are several lingering conflicts that have resulted from the perception that the college has “done nothing” in relation to protected actions by some within its constituencies. Additionally, security is aware that students in the emergency management program—which include a significant number of veterans and law enforcement-affiliated students—are feeling that the college is responding unevenly to some of the national events involving BIPOC individuals and the police.

Environment. The college is subject to U.S. state and federal laws related to harassment, discrimination, and Title IX. Faculty are also covered by a collective bargaining agreement and, consistent with academic institutions generally, enjoy broad freedom of expression under the concept of academic freedom.

Determination. The college holds monthly town halls for students, faculty, and staff. It determined that, on a quarterly basis, the college president will make the following points during his remarks:

The college is committed to diversity, explicitly including diversity of thought and expression.

Tolerance does not include tolerating the intolerable.

The college will not tolerate harassment or discrimination—as legally defined—and any staff, student, or faculty member who believes they might be experiencing it such should contact human resources or an office of student affairs.

When disagreements arise, individuals are expected to listen respectfully or disengage.

The college also determined that the diversity officer would create a reporting system for individuals who believed they experienced bias or microaggression, which a cross-disciplinary team would investigate. Additionally, the Title IX officer would partner with security to adapt the school's sexual assault bystander intervention program to train staff on ways to effectively intervene if they witness a disagreement devolve into an argument.

Finally, the college's chief academic officer and a few faculty members met with students from several programs, including emergency management, and scheduled a series of panel discussions involving law enforcement, local government officials, and community advocates to discuss local dynamics related to community policing.

MICHAEL CENTER IS THE UNITED NATIONS SECURITY ADVISER TO BELGIUM, FINLAND, GERMANY, IRELAND, MALTA, MONACO, NORWAY, PORTUGAL, SPAIN, SWEDEN, AND THE UNITED KINGDOM. HIS EXPERIENCE IS FOCUSED ON SECURITY RISK MANAGEMENT IN HIGH-RISK, COMPLEX HUMANITARIAN AND CONFLICT ENVIRONMENTS. AS THE UNDSS HEAD OF OFFICE, CENTER SERVES AS LIAISON BETWEEN THE UNITED NATIONS, HOST GOVERNMENTS, AND THE DIPLOMATIC COMMUNITY TO STRENGTHEN ANALYSIS AND CRISIS MANAGEMENT PREPAREDNESS FOR UNITED NATIONS PROGRAMS.

CENTER IS THE CHAIR OF THE ASIS INTERNATIONAL EXTREMISM AND POLITICAL INSTABILITY COMMUNITY. DIANA M. CONCANNON IS THE DEAN OF THE CALIFORNIA SCHOOL OF FORENSIC STUDIES AT ALLIANT INTERNATIONAL UNIVERSITY, WHERE SHE ALSO SERVES AS ASSOCIATE PROVOST FOR STRATEGIC INITIATIVES AND PARTNERSHIPS. SHE IS A FORENSIC PSYCHOLOGIST AND MAINTAINS A THREAT ASSESSMENT AND MANAGEMENT CONSULTANCY. SHE IS AUTHOR OF *KIDNAPPING: AN INVESTIGATOR'S GUIDE* AND *NEUROCRIMINOLOGY: FORENSIC AND LEGAL APPLICATIONS, PUBLIC POLICY IMPLICATIONS*. CONCANNON IS THE CO-VICE CHAIR OF THE ASIS INTERNATIONAL EXTREMISM AND POLITICAL INSTABILITY COMMUNITY.

THE VIEWS EXPRESSED IN THIS ARTICLE ARE THE AUTHORS' OWN AND ARE NOT REFLECTIVE OF THEIR ORGANIZATIONS.

SECURITY MANAGEMENT

Engaging Employees on their Mental Health

The mental wellbeing of the workforce needs to be a major consideration as organizations move forward after the turmoil caused by the COVID-19 pandemic.

By Scott Briscoe

There has never been a more important time to be mindful of the mental health of employees than now. After what organizations have endured during the past 18 months, it's remarkable that so many organizations can point to quick adaptation and resiliency on the part of their employees as amazing successes.

However, we may be seeing the costs that come with that success (see this ASIS-created infographic on mental health in the workplace). Last summer, the U.S. Centers for Disease Control and Prevention reported that 40 percent of people said they were struggling with mental health or substance abuse issues. The National Safety Council (NSC) reported that 9 in 10 employees said their workplaces caused them stress and 83 percent said they experienced "emotional exhaustion."

The Mental Health Index is a study led by management consulting firm Total Brain, along with partners that include the American Health Policy Institute and the HR Policy Association. The December 2020 Mental Health Index cited that the risk of general anxiety disorder had increased 80 percent. The index went further and conducted simple tests to see how these stressors affect people's cognitive ability at different points in time. From prepandemic 2020 until December 2020, the study showed a 9 percent decline in memory recall capacity and a 62 percent decrease in focus and sustained attention capacity.

From prepandemic 2020 until December 2020, the study showed a 9 percent decline in memory recall capacity and a 62 percent decrease in focus and sustained attention capacity.

"Our work and our workplaces impact our mental health and wellbeing," the NSC said. "This has never been more evident than with the changes in working conditions this past year—with some working from home indefinitely, some in extraordinarily high-stress and high-risk frontline jobs, often for longer hours, and others experiencing layoffs and job insecurities. ...Mental distress includes periods of intense nervousness, hopelessness, restlessness, depression, feeling like things require great effort, or feeling worthless or down on oneself. This distress is painful and costly for both employers and employees."

Even prior to the turmoil caused by the pandemic and civil unrest, a study from the United Kingdom's Institute of Occupational Safety and Health estimated that mental health issues cost UK businesses £42 billion ($58 billion) in lost productivity. Despite the costs, the same report found that 57 percent of people responding to the survey said their businesses offered no mental health or wellbeing training or support for managerial staff. Of the 43 percent that have some training, almost 80 percent reported that the training was not mandatory.

Just to pile on a little more, 80 percent of those surveyed said they would be reluctant to discuss their mental health with their manager. In an ASIS webinar in May, "Managing Better Conversations for Wellbeing," Heather Beach, founder and director of the Healthy Work Company, said employers have a duty to their employees to do better.

The good news is, as a manager you are not expected to be a caregiver.

"Quite often managers are promoted because they're very good technically at the job," Beach said. "They're not necessarily the best, empathetic people managers."

Beach said the context of this work duty does not just include severe mental health diseases, such as bipolar disorder, schizophrenia, or post traumatic stress disorder. It includes mental health issues that all of us experience. No human is immune to anxiety, stress, depression, or a host of other issues that can affect how people function, both professionally and personally. As the statistics above indicate, this is an especially acute time, one where managers—even ones with weak empathic ability—need to be sharp to ensure their teams are functioning well.

The good news is, as a manager you are not expected to be a caregiver.

"All you're expected to do is to notice that someone is struggling and have that conversation with them," Beach said, "to support them, to empathize, and to normalize, and to signpost them to get further support."

The NSC gives four recommendations for addressing employee mental health and distress:

Understand how workplace conditions and culture can impact employee mental health and, in some cases, create or enhance employee mental distress.

Ensure leaders, managers, and supervisors prioritize employee mental health and wellbeing; work to prevent mental distress; and support employees who experience it.

Ensure human resources develops robust, compassionate, and clear policies, programs, and procedures to prevent mental distress and support employees.

Provide employee education and increasing awareness on mental wellbeing and distress, as well as awareness of workplace resources, support, and policies.

"While understanding the impact of worker wellbeing on the bottom line is a critical motivator for organizations, we must be careful to not lose sight of the humanity of this issue," the NSC report said. "At the end of the day, we are all employees. We have all experienced unprecedented stress and distress over the past year."

Going from the organizational level to the individual level, in the ASIS webinar, Beach gives guidance for managers. She calls it the A-B-C-D approach. Here's a quick look at each component.

A – ASK

Managers who want to be in tune with the mental health of their staffs—all managers should aspire to this if they want to foster a high-performing team—need to be constantly aware. Managers need to be able to recognize behavioral changes. Did an employee who left at 5:00 p.m. on the dot every day suddenly begin staying later? Did someone who generally has an impeccable appearance show up to work a couple of times with a disheveled uniform? Has a generally passive employee become more assertive?

And when you notice something, ask about it. "Don't wait for the perfect moment," she said. "Especially now. There is no perfect moment is there? You might want to react quickly."

And, importantly, ask twice. Often the reflexive answer is that everything is fine, but if you ask twice, you are giving them permission to go beyond the expected answer.

B – BE PRESENT

If the ask leads to a conversation, it's time for managers to turn on the active listening skills. Humans are horrible listeners. In general, we hear a few thoughts and our minds begin racing, filling in all the spaces between the words the other person is saying with our own thoughts, suggestions, judgments, and—the worst—anything that we think makes us look smart or powerful. And then we can't wait to share these insights and we have quickly turned from trying to understand the person to whom we're supposed to be listening to thinking about how best to say back what we want to say.

Beach proposed that doubling down on active listening approaches is imperative in such situations. After all, as a manager you've done the hard work of initiating a conversation. It would be shame to wreck it.

Instead, summarize what they are saying using their words. Ask clarifying, open-ended questions to continue the dialog and improve your own understanding. Use and respect silence to encourage additional sharing.

C – CREATE A PLAN

The most important part of creating a plan in this context is that managers create a plan with the employee, not for the employee. In fact, the more the employee develops his or her own plan, the better. Remember the earlier statement from Beach: Managers are not expected to be psychologists, therapists, or parents. A manager's job is to support, to empathize, to normalize, and to help find or suggest additional support.

D – DUTY

Organizations have a duty to their employees. When managers engage employees in conversations about their wellbeing, Beach reminded that managers must remember their role in this. They are agents of the organization. That does not mean that managers do not also share the best interests of the employee. Quite the opposite, in fact, employees are also part of the organization. However, this dual role needs to be a factor in their conversations. Managers should not be promising confidentiality, for example. And managers should also document these conversations, even if it is in the form of contemporaneous notes that are not shared with anyone else.

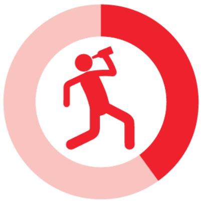
The goal is for managers to spot any issues quickly. It's true in so many situations: an early intervention can keep a minor issue from becoming a major obstacle. And that's often true with the mental wellbeing of employees. ▨

Mental Health Issues Are on the Rise

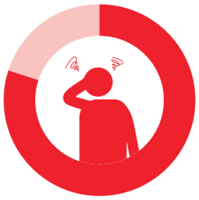
Risk of Depressive Disorder Increased

145%

Source: Total Brain, “Mental Health Index December 2020

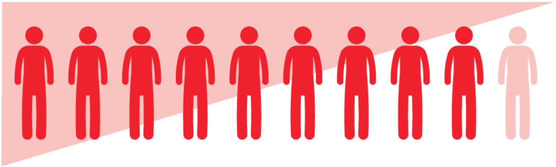


40 percent report they are struggling with mental health or substance abuse.



risk of general anxiety disorder increased **80 percent**

9 in 10



employees say workplace causes them stress, with 83% experiencing “emotional exhaustion”

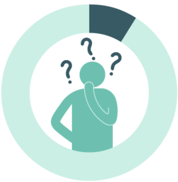
Source: National Safety Council, “What Employees Can do When it Comes to Mental Health”

57% **of workers in UK say their organization offers no mental health and well being training or support.**

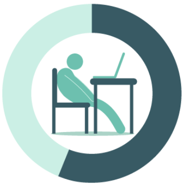
31% **of managers report being trained to recognize signs of poor mental health.**

Source: Institute of Occupational Safety and Health (UK), and Management Today, “Workplace Wellbeing”

Comparing Feb 2020 to Dec 2020



9 percent decrease in worker memory and recall capacity.



62 percent decrease in focus and sustained attention capacity

Source: Total Brain, “Mental Health Index December 2020”

An Organizational Approach to Mental Health

Starting Conversations

You have a duty of care to that individual

What you say and do matters

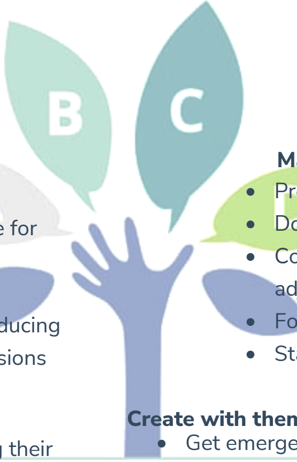
Consider when to signpost that person to an expert or someone else

You are not a therapist, life coach or doctor

You are not responsible for what they do and you cannot cure their problem

Consider if you are comfortable being available out of office hours or not

Awareness, Be Present, Create, Duties



Be Aware and Assess

- Increased absence for ANY reason
- Presentee-ism
- Difficulties in producing work/making decisions

Manager’s Duties

- Prevention-first approach
- Document conversations
- Consider reasonable adjustments
- Follow company procedures
- Stay in contact

Be Present

- Summarize using their words
- Ask clarifying/open questions
- Keep attentive eye contact

Create with them, not for them

- Get emergency help if needed
- Ask what they want, if they want help
- Find out who can help support the person

Self-Care Is Just as Important

spend time in nature
outdoors
TRY TO BE OPEN &
HONEST
reconnect to those close to you
start a new hobby
ADOPT A grateful MINDSET
FIND WAYS TO laugh MORE
savour the small things

Source: The Healthy Work Company

SECURITY
MANAGEMENT

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit asisonline.org/membership/join.