A companion eBook to
The Human Team®

The ABCs
of Preventing Loss & Elevating Performance



By Jeanet Wade
with Dave Chronister - Founder, Parameter Security

CONTENTS

The Connection Between HUMAN BEHAVIOR AND HUMAN NATURE 3

THE 3 B'S OF LOSS PREVENTION 7

A SECURITY EXPERT'S WORST NIGHTMARE 10
Contributed by Dave Chronister

THE 4 A'S THAT DETERMINE BOTH RISK AND PERFORMANCE 13

BAD ACTORS ARE NOT YOUR GREATEST RISK 15
Contributed by Dave Chronister

IT'S NOT ABOUT TRAINING, IT'S ABOUT CARING 20
Contributed by Dave Chronister

THE 6 C'S OF HUMAN NEEDS 23

CLARITY 24

CONNECTION 25

CONTRIBUTION 27

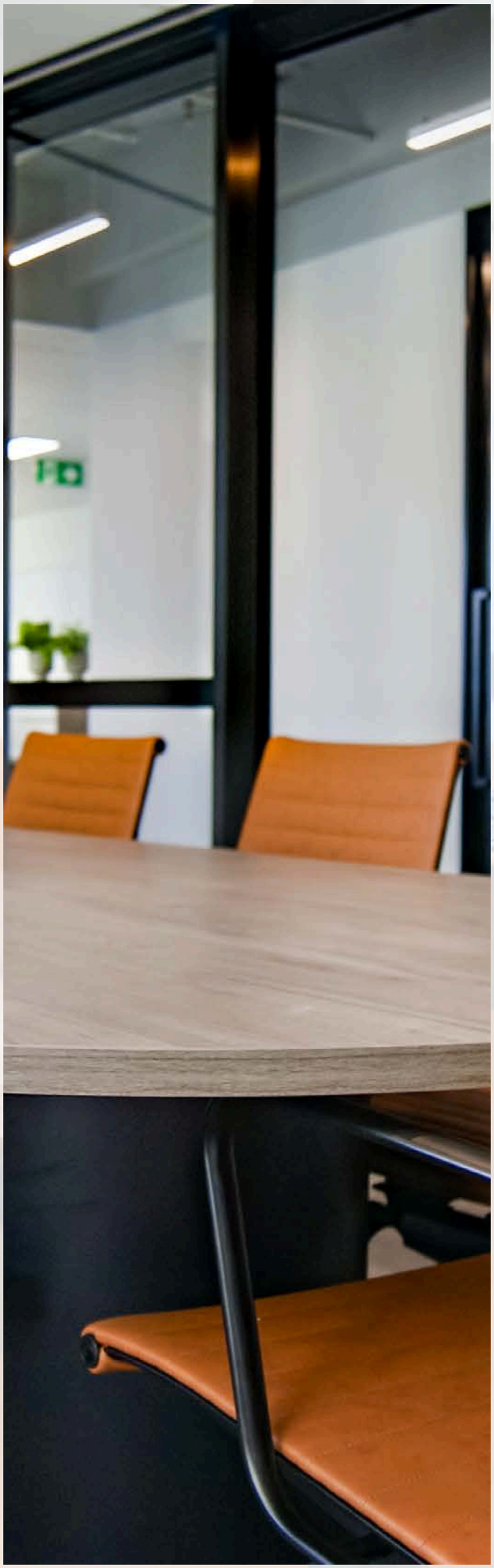
CONSIDERATION 29

CHALLENGE 30

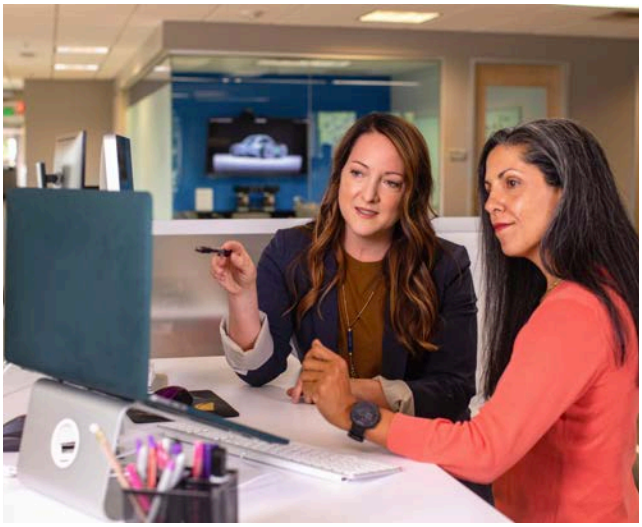
CONFIDENCE 32

THE FRAMEWORK AND FOUNDATION OF EXCELLENCE AND SECURITY 34

PRINT & SHARE THE SIX FACETS OF HUMANS NEEDS 36



The Connection Between Human Behavior and Human Nature



Have you ever tried to blow up a balloon that had a little tiny hole in it? Or drive on a tire with a slow leak? Or fill a glass with a hairline crack in the bottom?

Even thinking about trying to succeed under those conditions brings up the phrase "exercise in frustration" doesn't it?

That exercise in frustration is exactly what so many businesses are experiencing when they separate security and loss prevention from culture and team performance.

They're investing in elevating human performance but losing their return on that investment to everything from fraud and embezzlement to negligence and mismanagement of resources.

A couple of years ago, not long after *The Human Team; So, You Created a Team but People Showed Up* was released, I was asked to write an article about the connection between human nature and fraud for *Loss Prevention Magazine*.

Since that piece was published, I have had numerous comments and seen even more social media shares of the article saying that the connection between human needs and human behavior is something that has been sadly overlooked.

What has really been overlooked however, is that preventing loss is always about optimizing human behavior. And human behavior is always linked to human nature.



To expand on that article and on what I have observed and learned in the nearly two years since it came out, I invited my colleague and client, Dave Chronister, to add his 25 plus years of experience as the go-to expert in Cybersecurity issues and solutions in data, people, compliance, and physical security.

Dave is a forensic investigator and Cybersecurity Assessor and the founder and CEO of Parameter Security. He also appears regularly as a cybersecurity expert on Fox Business, CNBC, MSNBC, and CNN. You'll see Dave's contributions highlighted throughout this book.

Preventing loss is always about optimizing human behavior. And human behavior is always linked to human nature.

Let's start by looking at the more obvious forms of "loss"; fraud, petty theft, and embezzlement.

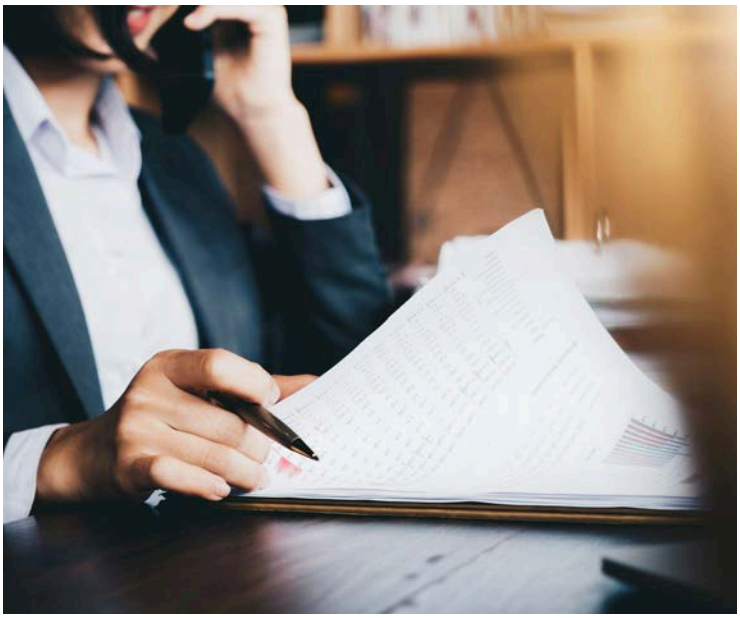
There are many ways your employees can steal from you. From the "borrowing" of office supplies to overreporting of hours, to embezzlement of money, divulging protected information, or selling intellectual property, there's no one with greater opportunity to help themselves to your company assets.

Small holes sink big ships, and those losses, even the minor ones, add up. In fact, an article from *CompareCamp* which provides an astonishing mash-up of statistics on employee theft, states that small thefts add up to 5% of revenue while inventory losses are as high as 43% of revenue in the US.

That doesn't even factor in misuse of benefits or other resources, over-reporting hours worked, or other fraudulent acts such as sale of data or company information.

Here's what the authors of that report give as the bottom line, "Potential global loss from fraud and employee theft is $2.9 trillion annually. It is also estimated that 33% of corporate bankruptcies in the US are linked to employee theft."

Yes, you read that right. That's trillion. With a capital T. Every single year.



And about 7,500 bankruptcies (there were 22,780 company bankruptcies reported in 2019) caused in part or entirely by employees stealing from their employers.

I won't quote that article further because one, you can read it yourself, and two, it gives me a headache just thinking about all the businesses being impacted by employee theft when so much of the loss could have been prevented.

Now when I say that some of the loss could have been prevented your mind probably goes to security measures, both physical and digital, and management oversight. But while those are important, and this book isn't intended to devalue diligence and enforceable security measures, those aren't your first line of defense in reducing loss due to occupational theft.

The best defense is developing a holistic plan around data, people, legal and physical requirements vital to keeping your business operational.

– Parameter Security

Security and management oversight are focused on reducing opportunity and recovering losses. Typically, when a company turns its attention to security the focus is on policy, detection, and enforcement. What policies must the company have in place, what checks and balances or visibility measures are in place to detect if policy has been violated, and what measures will be taken to enforce the policy?

If someone is tempted to defraud the company these measures may deter them, and if someone attempts a theft or succeeds in their efforts these measures may result in apprehending the thief and mitigating the damage. But how well do plans that depend only on policy, detection, and enforcement really work?

Want to know how many people have knowingly committed significant wrongdoing or been aware of a wrongdoing and haven't reported it? KPMG Forensic polled 3,500 U.S. employees for its Integrity Survey 2013. According to that report, 73 percent responded to that survey that in the last 12 months they had either committed or observed a serious offense.

This is where the connection between elevating human performance and preventing loss due to human behavior comes in.

This is where the connection between elevating human performance and preventing loss due to human behavior comes in. Your success in both of those areas will be determined by how well you are meeting the needs of the humans who work for your organization.

Before you shake that off as irrelevant, too vague, too undependable, too hard to measure or manage, or just too "touchy-feely" for your company culture, consider the two aspects of any crime – motive and opportunity.

Motive, of course, precedes opportunity. Without motive, crimes aren't as likely to be committed even when opportunity presents itself. And what security and oversight cannot do is to address motive.

But there is a lot you can do to address motive, and in doing so you'll also be taking steps to elevate the performance of the humans on your team.
It all starts with "knowing your ABC's."



The 3 B's of Loss Prevention

At the risk of getting our alphabet out of order, let's start with the three B's that influence the outcome when a person is faced with an opportunity to pilfer, defraud, or commit embezzlement or when they see or suspect that someone else is doing so.

BENEFIT

Because of course, for a person to knowingly commit an illegal or unethical act or look the other way when they see such an act taking place there must be some benefit.

Either the person benefits directly; financial gain, paid leisure time, "free" goods or services, or they benefit indirectly; avoiding the conflict or censure of reporting a wrong-doing, being in the "cool kids" who "get away with things" group, not exposing themselves to questioning from authorities.

To BEHAVE in an illegal manner they had to BELIEVE that the BENEFIT outweighed the risks and that they were, in some way, in the right even though their actions were, by society's standard, wrong.

BEHAVIOR

What does the person do? Do they take an action that is illegal and/or unethical? Do they take action to prevent loss or harm?



BELIEFS

Humans are fascinating. One thing that makes them so intriguing is their ability to hide their motives even from themselves and to create narratives to explain subconscious beliefs and emotions.

Beliefs, as we know, are often buried in the realm of the unconscious, meaning we may not know why we behaved in a certain way until the conscious mind is called upon to explain or justify our behavior.

In fact, we can, and often do, have conscious beliefs that are in direct conflict with an unconscious belief. So which belief will drive behavior?

MOTIVATION ISN'T ALWAYS OBVIOUS

Freud's "Iceberg Theory" held that the unconscious mind is actually the primary source of human behavior. Newer studies also suggest that indeed the actions of the unconscious precede the conscious.

Research posted in this abstract states that "several theorists have postulated that the conscious mind is not the source or origin of our behavior; instead, they theorize that impulses to act are unconsciously activated and that the role of consciousness is as gatekeeper and sense maker after the fact."



It's why, when we seek to elevate our own performance, we often turn to mindset coaching or hypnotherapy, because we know that if we "reprogram" the subconscious we will more easily create new behaviors that lead to desired outcomes.

But, as Dr. Maslow realized when he published his 1943 paper "A Theory of Human Motivation" in which he first shared the model for understanding the motivations for human behavior that we most commonly refer to simply as "Maslow's Pyramid", attempts at nurturing, consciousness reprogramming, or performance training are unlikely to achieve actualization of potential if basic human needs aren't met.

I have found that there is a similar framework that helps to understand the needs that must be met in order for humans to actualize their potential as part of a team, but we'll get to that framework when we get to the C's of the ABC's.

Let's go a little further in understanding how beliefs inform behavior in terms of motive for wrongdoing at work.

In the 1940's criminologist Donald R. Cressey studied the root causes of company fraud. Unsurprisingly he found that most of the nearly 200 convicted embezzlers he interviewed stole because of financial pressure.

However, he also found that there were two other determining factors for whether or not these employees went through with plans to steal from their employers. One, they had to have some belief that they were going to be able to get away with the crime. And two, they had to have a belief that their actions were justifiable.

So to take the illegal action that they did, they had to believe that the benefits outweighed the risks and that they were, in some way, in the right even though their actions were, by society's standard, wrong. Without those two beliefs they most likely would not have behaved the way they did regardless of their motivations.

BELIEFS AND MOTIVES

Beliefs can also provide the motive. We tend to think of motive in terms of greed, desperation, or just thoughtless pilfering. But studies show that for many employees who, when surveyed, admit to defrauding their employer, the motivation is discontent, feeling unappreciated, or simply a lack of engagement, loyalty, or connection to the company. Simply put, they believed that the company owed them something, or that the company deserved to lose.

Not all behavior that leads to loss is what we could call "wrongdoing." Rather it is a lack of "rightdoing."

In cases of petty theft, pilfering, time theft, or losses due to non-compliance the belief is often that it won't matter, it's a victimless crime, or that "everyone else does it too." They might even believe that management doesn't care, or that management is just as guilty (or more so) or even that a little "fudging" of the expense reports, time reports, or other documentation is expected.

As much as we try to balance the perceived benefits through threats of possible detection and punishment, it's really beliefs, conscious and unconscious, that are the greatest determining factor of behavior.

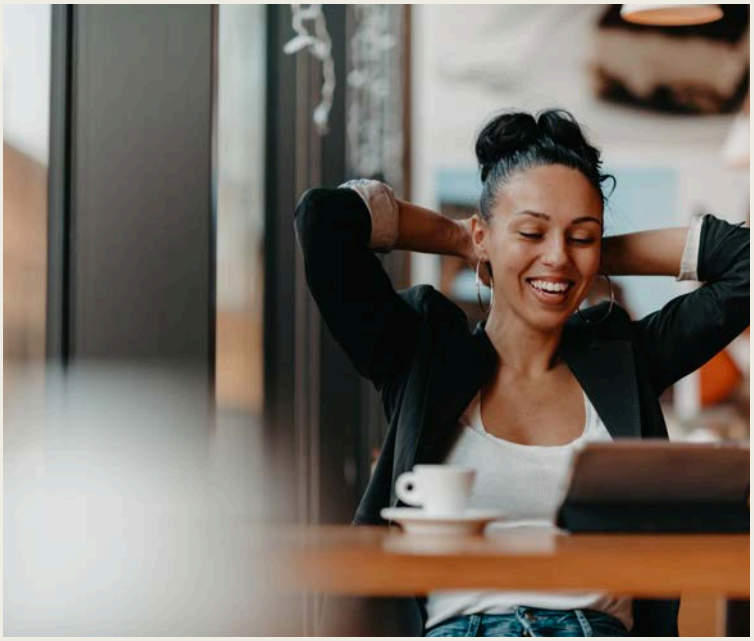
And not all behavior that leads to loss is what we could call "wrongdoing" but rather it's a lack of "rightdoing."

In loss prevention we know it is the engaged and motivated bystander who's most likely to prevent the crime.

A SECURITY EXPERT'S WORST NIGHTMARE

Dave Chronister - Parameter Security

In all the years I've been involved in testing security systems using everything from onsite surveillance to social engineering, I think the greatest risk factor and one that is usually overlooked, is whether or not people know how things should be and the right thing to do when they notice something that isn't the way it should be, and then if they do the right thing consistently and in a timely manner.



For instance, if every employee knows which doors should always be closed, and if they're motivated to take action when they notice a door being left ajar that should always be closed, they've just avoided a potential loss.

If people don't know how things should be, that's a training issue. But if they do know how things should be and they see something that is out of line with that standard and do nothing, that's a motivation issue.

"When we're invited to expose physical security gaps within a company our worst nightmare is the human being who's motivated to do the right thing."

Dave Chronister – Parameter Security

It's really what "The Finale" of Seinfeld was all about, the passive behavior of not taking action when action could have prevented a crime. In that two-part episode Jerry, Kramer, Elaine, and George stand by while another character gets held up at gunpoint. They record the incident, make fun of the guy for being overweight, but take no action to prevent the crime. They are then arrested for a violation of the Good Samaritan law called "duty to rescue" and end up in prison.

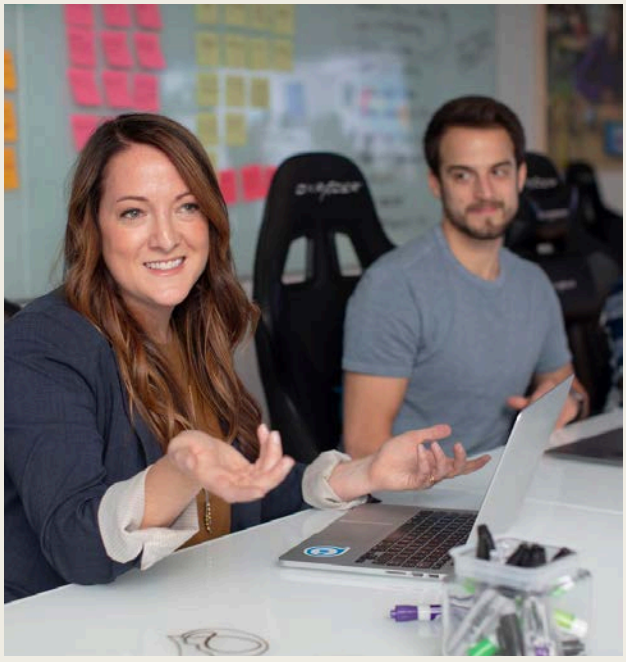
In loss prevention it's much the same principle; it's the engaged and motivated bystander who's most likely to prevent the crime. Of course, we aren't going to send the bystanders who do nothing to prison, but that doesn't mean they can't do a lot of harm.

One of the services we offer is on-site social engineering to test physical security. When we're invited to expose physical security gaps within a company our worst nightmare is the human being who's motivated to do the right thing.

It's the alert, caring employee who greets us with "How can I help you?" and means it. Because if we say, "I'm here to see So-and-So" they will walk us to that office. Which means we have no opportunity to do a little reconnoitering and infiltration along the way. Or they will ask us to have a seat and offer us coffee while they announce our presence to the powers that be. Helpful to the company, not helpful to us in our role as "bad actors out to steal anything and everything we can."

Seucrity measures can't make up for employees who are dissatisfied or disgruntled or even just disengaged.

It's always the visibly happy employees that have the greatest commitment to "helping" us. No matter how busy they seem to be, we know just by their attitude and voice tone that we aren't going to be left to our own devices that day.



On the other hand, when we walk in just trying to see what we can get away with because that is the whole point of the test, and we're greeted by someone who is clearly disengaged or overwhelmed or even disgruntled we can bet that we're going to have access to things no outside person should have access to.

The same is true when we're testing something like phishing, which is one of my specialties. An email with a suspicious link or from a suspicious source in a company where the team is cohesive and the culture is high-trust and open is going to generate questions.

Someone is bound to say, "Hey, did anyone

else get this email, it has a link that looks suspicious" or "I just got a weird email from someone who says they're a client" and off that email goes to be quarantined and blown up out there in the cloud where it does us (as the pretend "bad guys") no good whatsoever.

In a company where the culture is "who knows" or "who cares" or "just don't make waves," those links are likely to go unnoticed or at least uncommented on and they may even get clicked out of negligence or curiosity. And then, as they say, all hell breaks loose which is exactly the kind of opportunity we're trying to detect.

The bottom line is that, as a partner in identifying and closing security gaps, we can detect those kinds of opportunities and we can deliver strategies and technologies to close the gaps. But we can't make up for employees who are dissatisfied or disgruntled or even just disengaged. Creating a culture where employees know what they should notice and are motivated to notice and take appropriate action must always be up to our clients.

Those stories from Dave are so telling aren't they?

That in his long experience in uncovering all the ways that companies are vulnerable to security attacks it's the behavior of the humans working for the company that determines how easy his job as a "bad guy" is going to be.

We all know that prevention is always better, and certainly cheaper, than a cure, and a team of informed and engaged humans who are motivated to behave in a way that reduces risks and prevents loss is one of the best preventive measures you can take.

The 4 A's that Determine Both Risk and Performance

ATTITUDE

You've probably already guessed, because we all know how important it is in the workplace, that one of the A's is Attitude, which is kind of a catch-all for personality, values, preferences, and tendencies.

ACCOUNTABILITY

The second A is Accountability. Does everyone know the right thing to do and are they all willing to hold themselves and each other accountable for doing it?

Attitude and Accountability are two qualities we try to assess when hiring, and for good reason. People who rate high on both of these A's have the potential to be terrific team members *if* we give them the clarity and direction to live up to that potential.

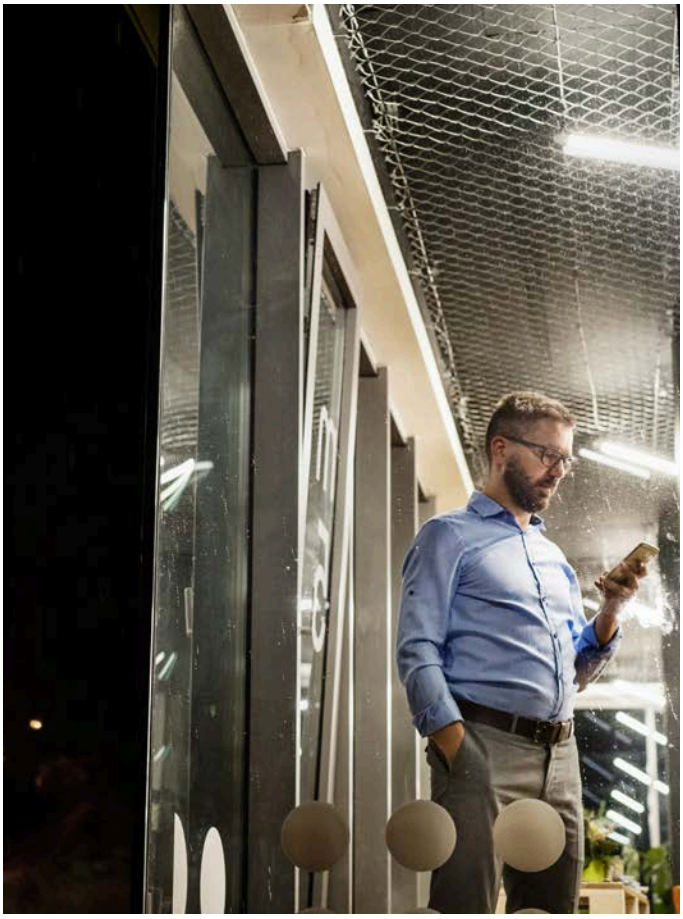
Unless you are extremely diligent or extremely lucky, not every human you hire has an attitude of accountability.

I remember a new client I started working with a few years back. They employed truck drivers and to be in compliance with the Department of Transportation the drivers had to keep accurate and detailed records of their activities. How many hours they were behind the wheel, how many hours they weren't driving, etc … It all had to be recorded in their log book and the log book had to be on file with their employer. Failing to comply with these safety regulations by not turning in their logs or turning in logs with incomplete or inaccurate information could have resulted in crippling consequences to my client.

Nonetheless, we discovered that the drivers weren't complying with regulations. Which puzzled me because they all seemed to have the right attitude. They were conscientious, engaged, well-intentioned humans who took pride in their performance.

When I brought this up in a team meeting I was surprised to learn that the drivers had been trained on the protocols, but they hadn't been informed of the penalties and sanctions their employer could face if they failed to follow them.

The drivers were stunned when we told them the potential cost of their non-compliance and quickly committed to getting their logs in order and keeping them that way. These were humans who had great attitudes and were willing to be accountable, they just didn't have clarity on the importance of what was being asked of them.



Of course, unless you are extremely diligent or extremely lucky, not every human you hire has an attitude of accountability.

As with most traits, conscientiousness tends to be a bell curve with a small percentage of people at one end who are so committed to doing what they perceive to be the right thing that they are likely to try to do so regardless of company culture or circumstances, and another small percentage of people at the other end so lacking in conscientiousness that they will actively look for opportunities to take advantage of others in big or small ways.

As with any bell curve, the largest percentage of people are somewhere between those two extremes.

Let's focus on the folks in the middle of that bell curve because that's your greatest area of risk and improvement.

Human negligence is the bane of every security system.

Bad Actors are NOT Your Greatest Risk

Dave Chronister - Parameter Security

The truth is that any security measure that one or more humans can create there will be another human who can figure out how to break it. There's no doubt there are bad actors out there, and sometimes companies make a mistake and hire one.

There are even folks who don't need much motivation to do really dastardly things to your company. They like the challenge, the thrill of getting away with it. Or they feel like the world owes them something. Or they think the company and the bosses got all the breaks and deserve to lose a little bit to the "little guy."



Our job is to make it as difficult as possible for anyone, maliciously or otherwise, to take any harmful action against the company. As I said earlier, we can't force a client to act in their own best interest and we can't change their attitudes or their culture. But quite often it isn't the bad actors who cause the most damage. It's the people who could take action to prevent that damage and do nothing or do something else instead.

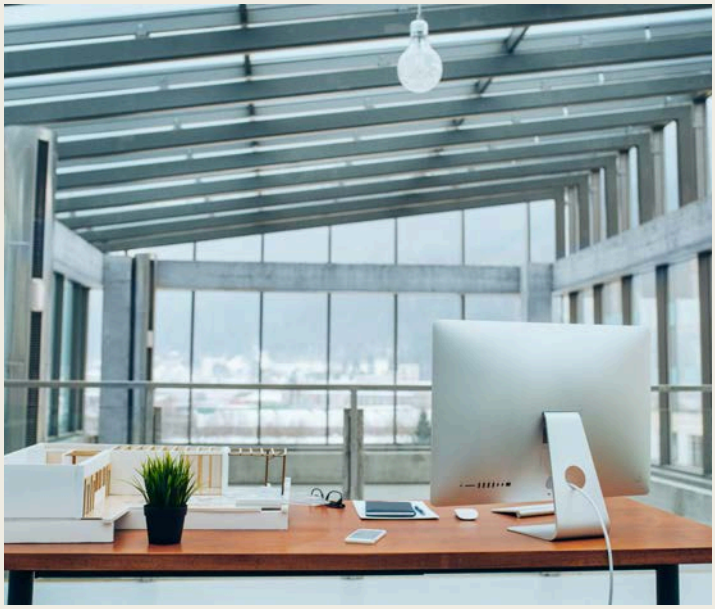
"Any security measure that one or more humans can create there will be another human who can figure out how to break it."

Dave Chronister – Parameter Security

One of the first on-site social engineering assessments I did after founding Parameter Security was for a credit union with three locations. The goal of the assessment was to see what sort of access I could get walking through the front door. In order for this to work, you create a pretext, or story explaining why you are there.

In this case I was a new pesticide company offering businesses free sprays to show how much better our product was. I was equipped with a sprayer filled with water, a spy camera, and a USB with "malware" which would connect back to our servers giving us access to the network.

I walked into the first location around 8:15 AM. I said "Bug guy, I'm here to spray" and one of the tellers said, "Do you want to start in the vault or offices". I was able to move around the bank without being accompanied. Within 15 minutes, using the USB, I was able to "infect" four computers. I left without any issues. Since I didn't use the pretext of being a new business offering free bug treatments at the first location and was able to get in, I decided to just pretend to be the regular bug spray company moving forward.



I went to the second location, walked in and said, "Bug guy, I am here to spray". The teller looked at me suspiciously and said, "You're not our normal bug guy, I need to see your ID." As I was in a different state and using a fake name, I didn't give my license, instead giving a fake business card.

The teller looked at it frustrated. She said to the teller next to her, "I ask for ID and this guy gives me a business card!" She then hands it back and sighs, "Come in" and opens the secure door.

While opening the door she makes the comment, "Sorry about being strict but we are a bank." I gained access to multiple computers with the USB and even found an unlocked computer which gave me access to customer's bank accounts.

At the final location I walked up to a part time receptionist, who was probably in her late teens-early twenties. When I say I am there to spray she askes if I had an appointment. I try my original pretext and she said I still need an appointment. The entire time she is actually being very pleasant and even helpful, telling me she knows they are looking for a new pest company.

But I can't get in. I finally let her know who I really am and she gets my contact, the president. I show him the video I took with my spy camera. When I show him the first location, he absolutely loses it. It ends up that location had been robbed for $20k the afternoon before. The president was at the location that morning telling everyone to be vigilant. I walked in not 30 minutes afterward and took over the network unopposed.

Now you may be thinking, "How stupid do you have to be?" But these weren't unintelligent people. You don't get to the level of success they'd gotten to without a brain.



They weren't stupid, and they weren't just overly trusting or they wouldn't have hired us in the first place.

What they were was negligent. And human negligence is the bane of every security system out there. It's the alarm that wasn't armed, the door that wasn't locked, the password that was written down or that hasn't been changed in a decade.

You can defend against bad actors. It's much harder to defend against people who don't do everything they know to do to keep the bad actors from taking action.

As Dave says, "The truth is that any security measure one or more humans can create there will be another human who can figure out how to break it."

It's also true that there are people who just don't have the attitude of accountability that results in following protocols and procedures. But even conscientiousness isn't a reliable predictor of behavior.

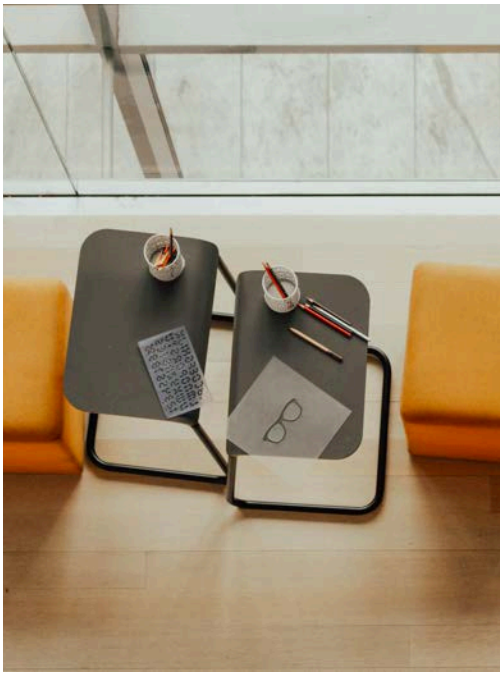
Unless you are extremely diligent or extremely lucky, not every human you hire has an attitude of accountability.

According to Kim Baker, Certified Reina Trust Building® Implementer and 6 Team Conditions Advanced Practitioner, research published in the "Journal of Occupational and Organizational Psychology" indicates that while people with higher levels of conscientiousness were more responsive to code enforcement, "Despite enforcement interventions to reduce workplace code of conduct violations, those low on conscientiousness and even 16% of those who measure high on conscientiousness committed workplace code of conduction violations which demonstrates that higher levels of conscientiousness mitigate but do not remove risk of workplace misconduct."

APATHY

Humans are complex beings and there are many factors at play in understanding the kind of behaviors that violate rules of conduct or ethics or laws. But one that I believe plays a very large role is our third A, Apathy.

You might think the humans on your team aren't apathetic because you see them excited about things, even passionate at times. But apathy isn't always a complete lack of emotion, it can also show up as an indifference or lack of concern about a certain thing. Mirriam-Webster describes it as "a lack of responsiveness to something that might normally incite interest or passion."



For most humans it's natural to be interested in, even passionate about, what they do for a living. They might be interested in the product or service they're helping to deliver, or interested in the activities that make up their day.

They might be interested in their status and success or in their ability to do their job to a high standard.

But a person who is apathetic toward the success of the company, the success of others on the team, and even their own success and achievements is perhaps the most dangerous employee you can have.

Not only will they not perform at their highest potential, they also won't provide that essential line of defense against theft, fraud, negligence, or other violations of company policy and code of conduct.
The apathetic team member isn't likely to notice when something is "off" and even less likely to take action if they do notice. They won't escort a visitor to the proper office or conference room or report the suspicious email. If they notice at all they'll likely shrug and file it under "not my job."

In that bell curve we talked about earlier, apathy creates a tendency for the behavior of those in the middle of the bell curve to slide toward the non-conscientious end of the spectrum.

Unless you are extremely diligent or extremely lucky, not every human you hire has an attitude of accountability.

ACTIVATION

The fourth A is how we can turn apathy around and create human teams that are emotionally connected to not only their own success, but the success of the company and their teammates as well. I call it Activation.

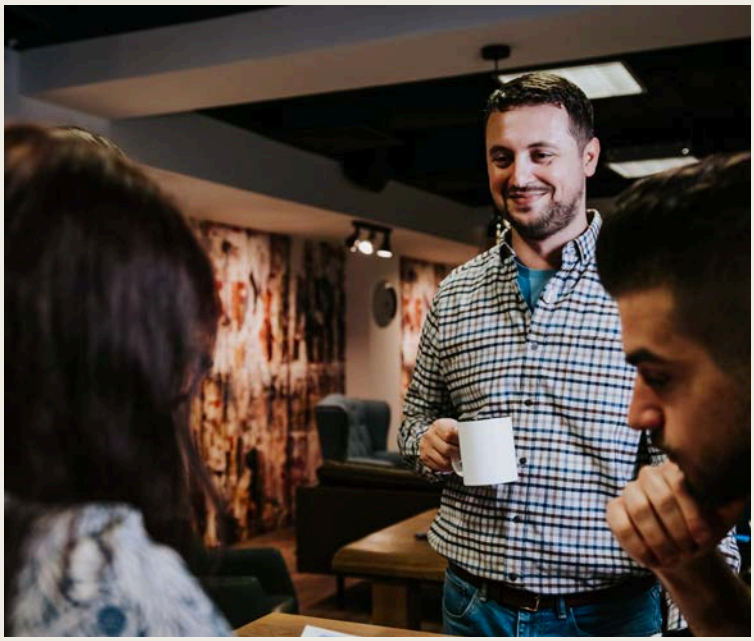
Activation is about tapping into human energy and potential, turning on striving instincts and leveraging human talent. It's about humans being emotionally connected, emotionally engaged, emotionally fired up and motivated. It's what we need to do as leaders to elevate human performance, but it's also what we need to do to prevent loss due to negligence and crime.

The easiest emotions to target are the negative emotions.

It's Not About Training, It's About Caring

Dave Chronister - Parameter Security

I've encountered about every kind of human in my years of being a security consultant. I used to say I didn't know which was worse, the employee who had no connection to the company or anyone they worked with and who was just in it to see how much they could get out of it, or the employee who had once been committed, motivated, and loyal and is now disillusioned and disengaged.



But really there's no competition. Because the employee who is just in it for themselves is going to be identified. It will be obvious that their attitude is a problem.

But the employee who came on board all gung ho and is now disconnected and apathetic is usually still doing their job well enough not to raise eyebrows. They may be whining and complaining a little, but they may not even care enough to do that. Surrounded by apathetic employees, a bad actor can get away with anything.

And the employee who was emotionally connected to the business and doesn't disengage their emotions when they get disillusioned is probably going to get disgruntled and resentful. Maybe even vindictive. And while they may never strike out in big ways they can do a lot of damage in little ways.

"Surrounded by apathetic employees, a bad actor can get away with anything."

Dave Chronister – Parameter Security

From being apathetic and taking no action, to being resentful and taking small actions, to taking criminal actions or falling prey to criminal actions, emotions play such a huge role in human behavior.

I used to give talks on psychology and social engineering and the big thing we know about why people fall for things like phishing is because of the knee jerk, preprogrammed, emotional reactions.

And really good cybercriminals know how to push the right buttons to get you to take the action they want you to take.

Most people like to think they're rational beings. And we do have this Dr. Spock analytical aspect that looks at everything and wants to analyze before taking action. But we also have this primitive animalistic emotional aspect. And when that gets engaged it trumps any language, any training, any logical or rational thought process.

Social engineering is how the cybercriminal knows what to say in the phishing email to make you feel instead of thinking. They don't need you to believe them or trust them, they just need to make you feel whatever it takes to get you to open that email, click that link, or enter that password.



The easiest emotions to target are the negative emotions. Get someone to thinking about how they're taken for granted, underpaid, underappreciated, overworked, etc … and their feelings of anger and resentment will easily override any caution. Get someone feeling inadequate or unliked and their feelings of self-doubt and shame will easily override training and logic.

It's the same phenomenon that makes someone buy the designer purse to impress their friends or continue to pay for someone's drinks even if they don't really like that person in hopes they'll be allowed to join the club.

We're all human and, as Jeanet would say, we all have "human moments." Even security professionals have been known to fall for a cybertrap. (Really, ask me how I know!)

If your culture is very isolating and critical, people don't feel connected to each other and they don't feel comfortable asking questions or bringing up a topic they know little about, it's easy to get people to fall for a phishing email. Their emotions are already primed, so to speak, and they don't have the emotional support of the team or management to bring the email to the attention of someone else or to make an informed decision about how to handle it.

On the other hand, if your culture is healthy and people feel safe asking questions or admitting to errors then even if they do open the email and click a malicious link they'll quickly report it and you can initiate damage control immediately.

Studies show that our behavior is influenced more by our feelings than by temptation. In an article titled "Why Employees Commit Fraud" the Journal of Accountancy summarizes one of the studies referenced in the article by saying, "The researchers concluded the most common reason employees committed fraud had little to do with opportunity, but more with motivation—the more dissatisfied the employee, the more likely he or she was to engage in criminal behavior."

Gallup estimates that actively disengaged employees cost US companies between $450 billion to $550 billion each year in lost productivity and goes on to say about those disengaged employees, "They are more likely to steal from their companies, negatively influence their coworkers, miss workdays, and drive customers away."

Activated employees on the other hand are engaged, connected, and motivated. This is the key to elevating performance, and it's also important to creating a culture where vulnerability to loss is reduced and potential loss or wrongdoing is quickly reported and damage control initiated without fear of reprisals.

Studies show that our behavior is influenced more by our feelings than by temptation.

Typically, when companies make employee engagement and emotional connection a priority they turn to nurturing and bonding activities. And they may see a temporary bump in morale, but unless there are systemic changes made in conjunction with these activities the increase in engagement is likely to be short-lived and may even backfire.

That's because, before we can nurture people to excellence or even engagement, we must meet their natural, universal needs as human beings. Nature – our instincts, brain function, and what Kathy Kolbe, theorist and founder behind the Kolbe® Conative Assessment tool, calls "MO" or modus operandi – is at the core of our most deeply ingrained beliefs and behavioral patterns. Nurture – the activities of coaching, engagement, and motivation – cannot take root until we've accounted for nature.

The bridge between nature and nurture is to understand and provide what humans need in order to be fulfilled or "self-actualized" as part of a group dynamic. These, in The Human Team®, I call The Six Facets of Human Needs®. This framework allows business leaders to dependably assess their team health and create processes and structures to meet these human needs in order to increase employee engagement and satisfaction, elevate performance, and reach the potential inherent in each individual human being who is part of the team.

THE SIX Cs of HUMAN NEEDS

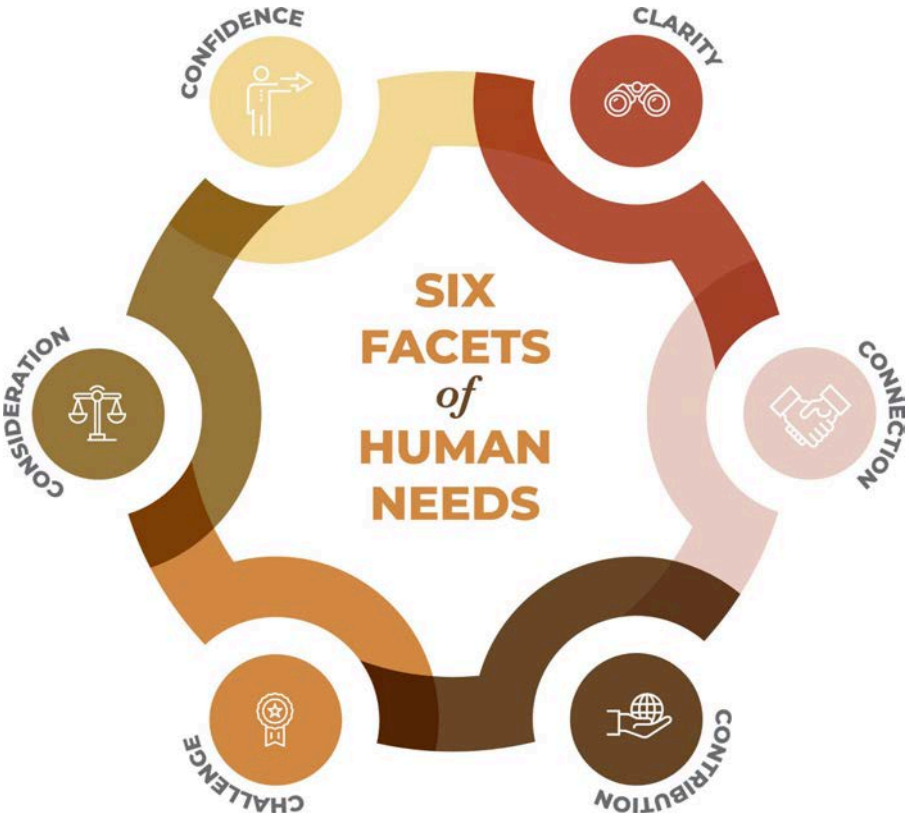
Now we come to the Cs of the ABCs of Preventing Loss & Elevating Performance. There are six.

We often refer to The Six Facets of Human Needs® as "the six C's" because they all begin with the letter C.

- Clarity
- Connection
- Contribution
- Consideration
- Challenge
- Confidence

Each of these C's is an essential element or "facet" of meeting human needs and activating human potential.

But as you can see from how each C relates to what we've already discussed about loss prevention, they're also instrumental in building teams that are a great line of defense against criminal, unethical, negligent, or simply unintentional harm.



CLARITY

When we lack clarity we either become reluctant to take action, we try to bluff our way through taking action in spite of our confusion, or we mistakenly think we're clear and take action that's based on inaccurate or incomplete information.

Just as Dave pointed out, it's the motivated employee who knows how things should be, notices when something is out of line, and takes action to correct the situation that is the bad actor's worst nightmare. But if that motivated employee lacks clarity about how things should be, or about the action that needs to be taken, their motivation will dissolve into frustration at their inability to do the right thing at the right time.



CLARITY

True clarity about everything from the big vision, to roles and expectations, to company and individual goals results in a team that can be effective even when they have to navigate conditions that are uncertain or ambiguous.

My client's employees who weren't in compliance with their log books had the right attitude and accountability, but they weren't clear on why compliance was so important and the risk non-compliance represented. Once they had clarity they were committed to being in compliance.

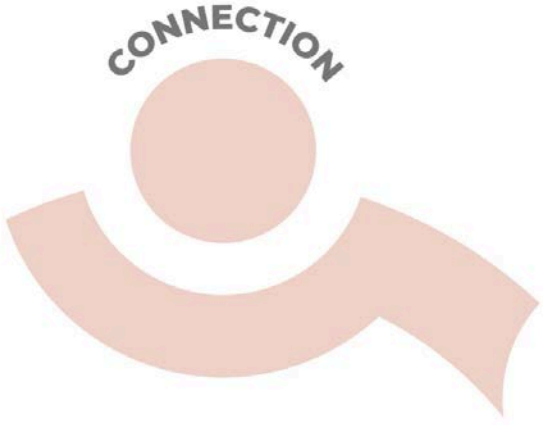


The human need for clarity goes beyond training or documentation, it's centered in needing to understand what we can expect and what others expect of us, needing to know what is considered appropriate and what is likely to be frowned upon or censored. We also need to have clarity of purpose, what is the mission and vision we're part of, why are certain things more important than others, and what opportunities will we have to deliver value, create impact, and be rewarded.

CONNECTION

We can see in Dave's examples so many ways that behavior that resulted in loss came from humans who didn't feel connected to each other, to the company, or to the mission or desired outcome. But when the people were a "cohesive team" the actions they took made it more difficult for the "bad guys" to win.

As humans, we are basically herd animals, wired for connection and belonging to understand ourselves and to feel safe in the world.



CONNECTION

Humans have a basic survival need to feel connected, to have a sense of belonging to a group of people who share something bigger than themselves.

The areas of the brain activated by feeling "othered" or disconnected are the same as those activated by physical pain.

When people feel disconnected, excluded, or alienated in a group setting they are likely to develop a "me versus them" belief system that can easily degenerate to seeing the company as an adversary. But when they have a sense of connection they see themselves as part of the company and identify the success of the company with their own level of success.

The effects of connection go far beyond psychology or self-reporting studies. Research on the neurological changes in the brain brought on by connection or by "othering", the process of identifying yourself or others as part of the "in group" or the "out group, show that the areas of the brain activated by feeling "othered" or disconnected are the same as those activated by physical pain.

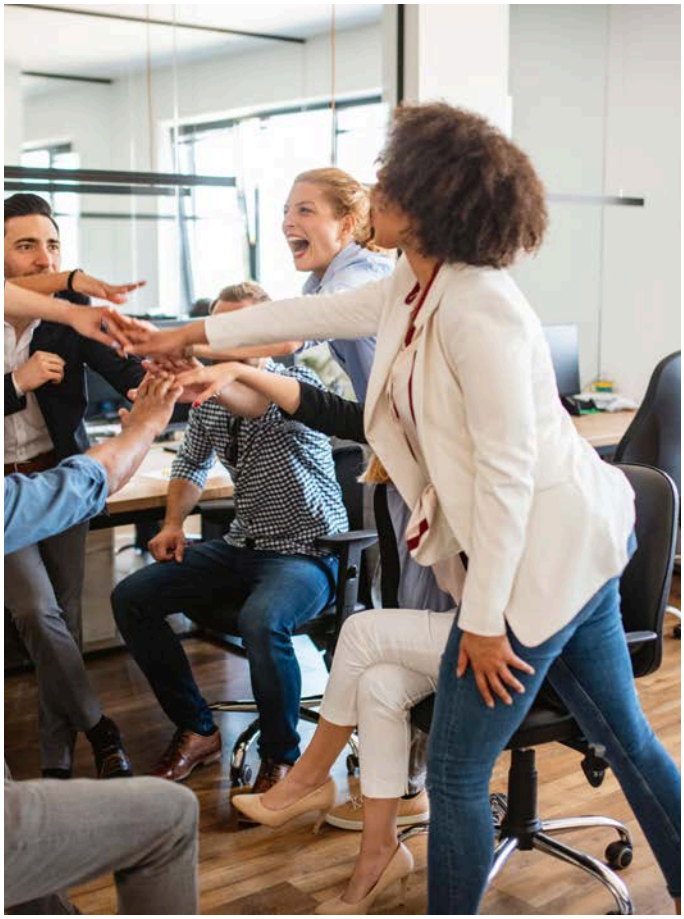
On the other hand, feeling connected or part of the group resulted in an increase in oxytocin, the love hormone, or "cuddle chemical", which bonds us to people and promotes human connection.

Meeting your teams' need for connection is more than building personal bonds. In fact, having individuals who feel connected to some of their teammates but not to the company as a larger idea is likely to result in subgrouping which can increase feelings of othering and lead to destructive behaviors.

To have a true sense of belonging the humans on your team need to feel connected at several levels.
Yes, they need to feel connected to each other.

They need to have a sense of community and that a win for the company is a win for all the members on the team. In order to connect with each other at that level they also need to connect to the bigger concept of what the company stands for – the mission, values, and culture – what beliefs and ideals hold you all together.

And finally they need to connect to the company's place or space. In human evolution geographic spaces were critical to belonging to the tribe and that sense of being connected through sharing physical space is still wired into our DNA.



The truth is that most people don't harm people or things they feel connected to or a part of. Of course, there are exceptions, desperation or disregard for others are factors that can certainly override those norms. But you can certainly reduce the number of employees who would be able to rationalize harming the company just by increasing their level of connectedness to the company.

CONTRIBUTION

One of the most important things we can do as business leaders, both in terms of creating healthy, productive teams and mitigating risks of employee theft, is to acknowledge the human psyche's need to contribute and reward those contributions.

The people who are a security testers "worst nightmare" as Dave described them are the ones who know how to make a contribution. They may not see it as "loss prevention" but their contribution to service, to taking good care of the visitor, or their diligence in making sure that anyone on the premises is not left unattended to get lost or find their way to a place they should be is a way of contributing to the best scenario for all concerned. (Unless you're the "bad actor" who's trying to get away with a crime, in which case it's not the best scenario you imagined for your purposes.)



CONTRIBUTION

Humans love to contribute. It's what we contribute that creates value in the world, that validates us in our own eyes, that offers fulfillment and accomplishment.

When we don't feel we are making a meaningful contribution it's human nature to disengage. Have you ever found yourself sitting in a meeting, mind wandering, toes tapping, trying to figure out your purpose for being in the room or on the call? How engaged were you, and how much attention did you give to the proceedings of the meeting?

If we want healthy, engaged, loyal teams we have to allow them to contribute at the highest level of their capability. Anything less and, as you probably noticed if you reflected on the scenario above, they begin to disengage. And that disengagement isn't confined to the context of that single meeting.

People who feel insignificant or undervalued will either disengage, leading to lack of connection and resentment, or in their desire to be significant and a part of the project or objective will disrupt those who are currently contributing at a higher level.

Either outcome leads to business loss and increased risk.



To make sure everyone feels their contributions are meaningful and valued ask yourself the following questions:

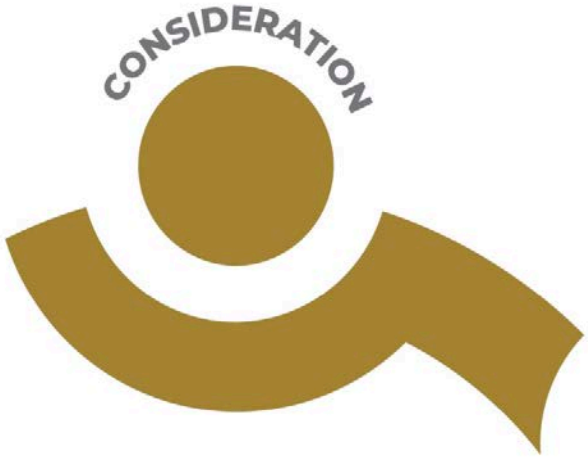
1. Is everyone on your team serving at their highest and best?
2. When setting expectations, are you achieving mutual agreement?
3. Does each team member have a voice at the table? Do you have the right voices at the table?
4. Is each individual continually learning and then applying new knowledge to the team or organization?
5. Does the team member feel they are contributing meaningful work? Do they like their job and/or role?
6. Have you established guidelines for working as a team?

Finally, pay attention to the size of your teams. Smaller teams increase engagement and allow greater contribution from everyone included. Studies show that small-team intimacy triggers oxytocin and increases empathy. It's probably the reason that Amazon founder Jeff Bezos goes by the two-pizza rule. If you can't feed a team with two pizzas, he says, it's too big.

CONSIDERATION

Every human wants to be valued. And we know when we aren't. A person who senses that they are unappreciated, inadequately compensated (and not all compensation is monetary), or treated unfairly in any way is going to be tempted, consciously or not, to balance the books so to speak.

As Dave pointed out, the people most likely to become apathetic or disgruntled enough to take harmful action even in small ways, often started out as gung-ho committed employees. But because they didn't feel valued, appreciated, and considered their attitude changed resulting in potential loss to the company.



CONSIDERATION

Consideration refers to making people feel seen, heard, and appreciated. It's both about how each person on your team feels and how they make others feel.

And that's the key to consideration, that we begin by recognizing and respecting the unique human being, that we apply the "Platinum Rule" of treating them the way they want to be treated, and that we reward contributions appropriately, which can range from a high five, a public thank you, a small gift or card, or a monetary reward such as raise.

When people aren't having their need for consideration met they feel like a "non-entity", no more individual or important than a robot or a cog in the wheel. Their self-esteem plummets, and because, historically, unimportant members of the tribe weren't as likely to be protected by the tribe, their biological sense of safety is threatened.

And when our significance and survival feel threatened it's easy to rationalize a preemptive strike. Or to bond with other discontented people in the "tribe".

To meet the need for consideration, build a culture where people are seen as unique and valuable human beings before they're categorized for their skills and capabilities.

Make sure leaders and managers are getting to know the people whose success they're responsible for. Small gestures like knowing which baseball team someone follows or what college their kids go to will go a long way toward establishing your consideration for them as a human being.

When people aren't having their need for consideration met they feel no more individual or important than a robot or a cog in the wheel.

Showing genuine consideration for the people on your teams has actually been shown to be more motivating, and to build greater loyalty, than even monetary incentive programs. And it's certainly more cost effective than trying to recoup losses from employee theft, fraud, or underperformance.



CHALLENGE

As I mentioned at the beginning of this article, loss prevention is as much about focusing on incentivizing people to do the right thing as it is about making it difficult or unprofitable for people to do the wrong thing. And one of our greatest incentives to do the right thing is because it feels good, not in a moral self-righteous way, but in an emotionally satisfying, fulfilling kind of way.

It might seem counter-intuitive, but I'm sure you have observed it in yourself and others, that when we feel challenged to be our best self, to rise to our potential, and to be of the highest benefit to others we have an emotional stake in the outcome of that challenge.



CHALLENGE

It's when we're challenged that we often come alive. We engage in a process of practice and improvement that will lead to true mastery. We're inspired to innovate, and to strive toward higher and higher goals.

I noticed that in myself when I accepted the challenge to step into a more challenging role as an EOS® trainer and community leader. While I have been involved with EOS® for over a decade, and have always felt a high level of loyalty and investment in the success of the company and my colleagues, this new level of challenge gave me an even greater sense of emotional ownership.



One of the fundamental tenets of EOS® is "do the right thing." And I'd always tried to live by that principle, in fact it is one of the things that made EOS® so attractive to me from my first encounter with it. But once I'd accepted this new challenge I found I felt even more empowered and inspired to practice it.

Faced with a dilemma of speaking up or shutting up, it was an even easier, more obvious course of action to choose the option that felt most "right" for the company and all involved. The challenge of stepping up, being an "official" example to my peers and colleagues, being invited to live up to greater levels of performance and potential resulted in an even greater emotional incentive to "do the right thing."

And that is just human nature. Most of us, when we accept a challenge, are invested not only in our personal success, but in the success of the endeavor, whatever it may be. And no one wants to see something they are emotionally invested in sabotaged by anyone or anything. So we're more likely to speak up when something "just isn't right" as well as when something is clearly, criminally wrong.

CONFIDENCE

In the context of activating human potential on a team, confidence goes beyond personal confidence in our own abilities. What we need as part of a team is to have confidence in the abilities and intentions of those on whom our success also depends.

It's this kind of confidence that makes it easier for people to do the right thing and harder for those individuals who are intentionally trying to do harm.

We need to have confidence in our leaders and managers, not only that they can do what needs to be done to help us learn, grow, perform, and be fairly treated and compensated, but that the intention and followthrough is there to actually do those things.

We need to have confidence in our co-workers that they not only have the ability to do their work well, but that they have the intentions and follow through to perform at the highest level possible in their role.



CONFIDENCE

There's nothing like the feeling of real confidence to make us feel motivated and alive! When you increase the confidence of your team you'll create a growth-mindset organization that is able to run on all cylinders.

It is this 360 degree confidence that creates a synergistic effect for human teams and propels individuals to a level of performance far above what personal confidence in themselves could achieve.



It's also this kind of confidence that makes it easier for people to do the right thing and harder for those individuals who are intentionally trying to do harm.

An employee who has confidence in their managers and teammates won't hesitate to report something suspicious because they know they won't be penalized if it turns out not to be an issue and they won't be ostracized for "outing" someone who is doing something unethical or illegal. They will have the confidence to quickly own up if they've made a mistake like clicking a link in a phishing email because they know that mistakes are forgiven and measures will be taken to mitigate any damage caused.

If people don't have that kind of confidence it's natural for them to second guess their instincts if they think something is just "off" or to avoid reporting when it could cost them status or credibility or the goodwill of their managers or peers.

THE FRAMEWORK AND FOUNDATION OF EXCELLENCE AND SECURITY

These six C's are the framework and foundation on which we can build teams of humans who are activated and engaged in reaching their potential. And they're also the key to building your first and strongest line of defense against loss.

When you contrast the beliefs and emotions of someone who feels connected to the people they work with, the company they work for, and the mission and values the company represents, to someone who feels disconnected or even excluded from the groups and structures in the workplace it's obvious that it's easier for the employee with less sense of belonging to rationalize wrongdoing.

The bottom line is, when you put your focus on team health and elevating team performance, risk mitigation is just a welcome byproduct.

The same is true when you think about the employee who knows they are considered to be inherently valuable as a human being as well as an asset to the team versus someone who feels like a "plug and play" robot or a cog in the wheel.

And certainly, it's hard not to understand that someone will be more protective of the success of the company when that success represents their own contributions and those contributions have been validated and valued.



The employee who feels disconnected or excluded, like an unimportant cog in the machine whose contributions are minimal or unappreciated can easily rationalize looking the other way when they see unethical or even illegal behavior.

And they're more likely to rationalize committing those acts themselves.

On the other hand, the person who feels as though they belong and play a vital role in something bigger than themselves, who feels like they are seen, heard, respected, and rewarded for their contributions, actually identifies as a part of the company – they feel any harm done to the business as personal to themselves.

The bottom line is, when you put your focus on team health and elevating team performance, risk mitigation is just a welcome byproduct.



If you're ready to reach for resources to speed up your growth you can:
read the post *10 Ways to Activate the Potential of Your Human Team*,
download the *free assessment and previous ebooks*,
or contact me for more information on how to
create self-actualized teams of humans that not only produce more, innovate more, engage more, and ultimately create more value during the time they are employed, but also experience greater fulfillment and satisfaction as a result.

Print & Share

THE SIX FACETS OF HUMAN NEEDS®

#1 CLARITY

True clarity about everything from the big vision, to roles and expectations, to company and individual goals results in a team that can be effective even when they have to navigate conditions that are uncertain or ambiguous.

#2 CONNECTION

Humans have a basic survival need to feel connected, to have a sense of belonging to a group of people who share something bigger than themselves.

#3 CONTRIBUTION

Humans love to contribute. It's what we contribute that creates value in the world, that validates us in our own eyes, that offers fulfillment and accomplishment.

#4 CHALLENGE

It's when we're challenged that we often come alive. We engage in a process of practice and improvement that will lead to true mastery. We're inspired to innovate, and to strive toward higher and higher goals.

#5 CONSIDERATION

Consideration refers to making people feel seen, heard, and appreciated. It's both about how each person on your team feels and how they make others feel.

#6 CONFIDENCE

There's nothing like the feeling of real confidence to make us feel motivated and alive! When you increase the confidence of your team you'll create a growth-mindset organization that is able to run on all cylinders.





JEANET WADE

Expert EOS Implementer® | Business Alchemist | Author

As one of the the first EOS Implementers® to earn the "Expert" designation, and the founder of Business Alchemist™, Jeanet Wade has helped businesses struggling with complexity and leadership alignment to become focused as a team on outcome achievement.

She has successfully helped leaders create environments of action as they execute and implement strategic growth initiatives. Jeanet's passion is helping entrepreneurial leaders of privately-held companies get what they want from their business – profitable growth, effective and accountable people, and more control of the business, so the business is no longer running them. Authoring the bestselling book, *The Human Team® - So You Created a Team, But People Showed Up!* came out of that passion and her 650+ on-site days of working with leaders to achieve that goal.

Jeanet's focus is always on building healthy teams and healthy bottom lines. She developed a reputation for helping clients get Traction® on their Vision by leveraging her experience in marketing, innovation, and management. Because of her passion for people and insights into the basic human needs that must be met in order to fully actualize the potential of a team, she quickly became known as the go-to resource for how to have effective, healthy team dynamics that allow the business to harness their people energy and maximize their "Return on Individual."

Cutting his teeth on technology starting at age 5, Dave gained an instant attraction to the inner workings of his computer. Before the age of 8, he wrote his first computer software program and, by the time he was a teenager, he ran one of St. Louis' biggest networked bulletin board systems. One of his favorite movies is WarGames, which he believes captures the life of a hacker accurately. Dave's interest in information security grew from that point on.

Dave has experience in several different technology positions that has given him a broad view of the field. He worked as Architect for A.G Edwards' electronic messaging system, as a technical liaison to credit card organizations, as a HIPAA compliance technical advisor for medical and dental practices, and as Chief Technology Officer for a $700 million dollar bank holding company.



DAVE CHRONISTER

CISSP, CISA, CISM, PCI-DSS QSA
Founder & CEO Parameter Security

He then went on to found Parameter Security in 2007, which has grown into an information security company offering a large array of assessment, advisory, and DFIR services regarding InfoSec technology and policy. Dave enjoys speaking about these topics —he has traveled to over 22 countries for conferences and training events!

Dave has appeared on several news programs including on ABC, Fox Business, CNBC, MSNBC, and CNN, as well as on local radio stations. His work has appeared in multiple online and print publications including Popular Science, Associated Press, Information Security Magazine, FOX Business News, and CBS. Outside of work, Dave enjoys spending time with his family, playing guitar, and listening to SCI-FI and Fantasy audiobooks.