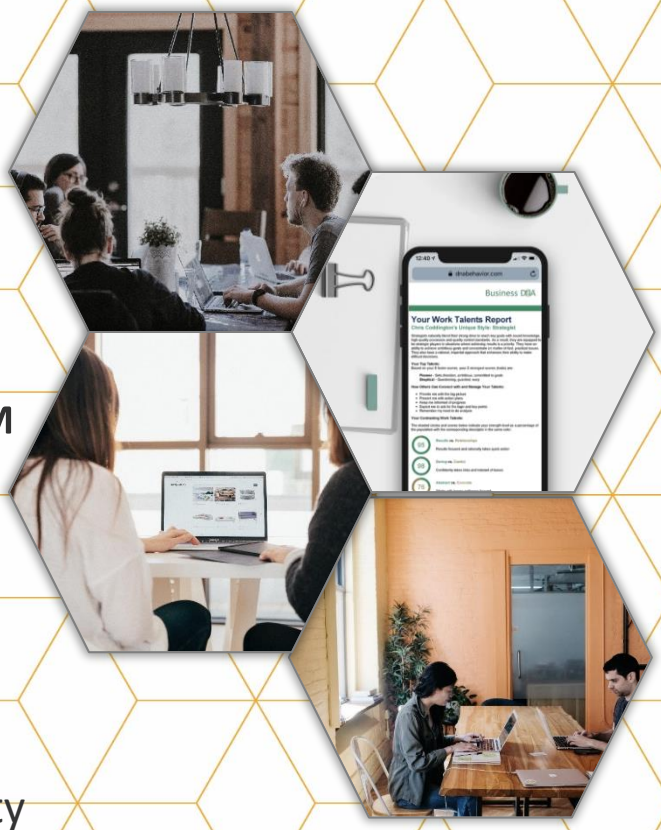


Behaviorally SMART™ Operational Risk Management

Predicting and Managing Employee Security Risks Using Behavioral Science

DNA Behavior®

DNA Behavior®

BEHAVIORALLY SMART™ OPERATIONAL RISK MANAGEMENT

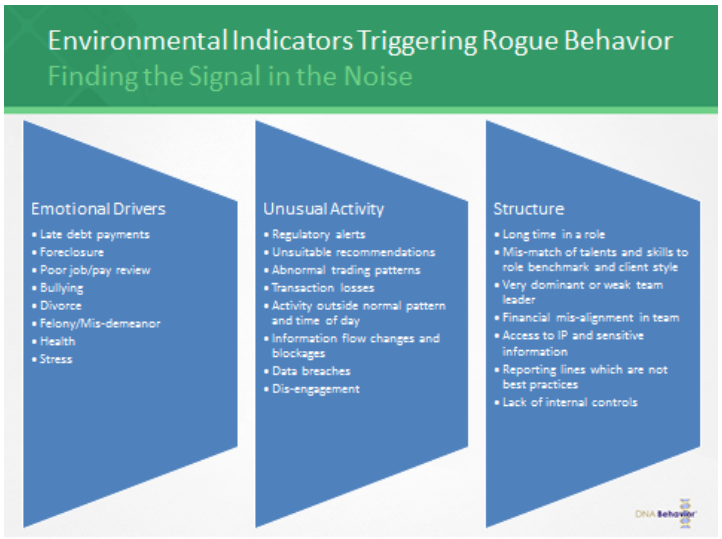
Identifying the Enemy Within

Potentially 5% of your workforce includes employees who could be a high security risk if not monitored.

Do you know which employee is potentially a "Molotov Cocktail" for your business?

Business leaders (starting with the Board) need to face the fact that people when placed under significant pressure react in ways that can prove costly at best and disastrous at worst for companies. For instance, a quiet and mild-mannered person could become aggressive; those who are spontaneous and happy go lucky could become random and erratic: those normally able to take measured risk become volatile and unstable in their decision-making.

The degree to which these behaviors will manifest is not necessarily dependent on high pressure points or major changes in an organizational structure. They can be activated when two colleagues can't work well together or when outside environmental influences are driving behaviors in the workplace.



The general approach to protecting businesses has been to monitor tasks such as phone calls, inappropriate use of internet, social media usage, medical absence records, etc. All of these have a place in securing the business of an organization but fail to drill into what is happening below the surface of an individual.

All the monitoring available will not predict inherent behavior that given certain environments could erupt and place your company at risk.

DNA Behavior®

According to validated research there is no easy way to detect threats where the past doesn't predict the future.

How Real Is the Threat?

In many organizations, protecting the tangible assets and intellectual property tends to be the major source of any investment to secure the business. In reality, a rogue insider has the potential to cause significant damage to the organization and as an insider, often with privileges, has many advantages over an attacker from outside the organization.

At the center of every security incident and breach is a human being; someone whose behavior could have been predicted.

▪ 75% of insider incidents are not detected or reported. (FBI) 2014 US State of Cybercrime Survey, cosponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014 ▪ 88% of privileged users said they "wouldn't recognize specific threats.http://www.ponemon.org in association with IBM ▪ 32% of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders. 2014 US State of Cybercrime Survey 2014 US State of Cybercrime Survey, cosponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014	▪ 90% of cases can't be detected by malware. "It's a people-centric problem." ▪ Insider threat is not a technical or "cyber-security" issue alone. ▪ A good insider threat program should focus on deterrence, not detection. ▪ Detection of insider threats has to use behavioral-based techniques. ▪ The science of insider threat detection and deterrence is in its infancy.Kate Randal. Insider threat analyst. FBI. *Combating the Insider Threat: Real World Lessons, RSA Conference 2013* ▪ The percentage of incidents attributed to current and former service providers, consultants, and contractors increased to 18% and 15%, respectively, in 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Insider Threat

- Current employees 35%
- Former employees 30%
- Current service providers/consultants 18%
- Former service providers/consultants 15%

- Suppliers/business partners 13%
- Customers 11%

http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Companies that fail to continually watch for employee and executive fraud typically lose 5% of revenues each year to insider cunning, which amounts to nearly $3.7 trillion globally.

2014 Global Fraud Study by the Association of Certified Fraud Examiners (ACFE)

80% of the fraudsters are first-time offenders who have worked at the company for years. Two-thirds are male.

2014 Global Fraud Study by the Association of Certified Fraud Examiners (ACFE)

Conspirators tend to steal more than individuals.

http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

77% of the frauds were committed by individuals working in one of seven departments: accounting, operations, sales, executive/upper management, customer service, purchasing and finance.

http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

23% of Annual spend should be directed to Behavioral profiling and monitoring.

The Global State of Information Security Survey 2015

30% of insiders take data to start own business

David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

65% take data to seek work with a rival

David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

72% of security incidents at financial services organizations involved current or former employees.

David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

Trusted 3rd parties responsible for 41% of the detected security incidents at financial services organizations.

David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

62% of security incidents at industrial product organizations involved current or former employees

David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

In US healthcare the top 3 perceived threat motivators by employees:

Accessing relatives/friends data (80%).

Financial identity theft (66%)

Identity theft (51%).

David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

Cost of Security Breaches

Regardless of whether negative deviance is overt or implicit, it can have devastating consequences for the business and its affiliates. The estimated impact of the widespread theft by employees on the US economy has been reported to be $50 billion annually. Toxic organizations depend on employees that are dishonest and deceitful in order to be successful. Source: Positive and negative deviant workplace behaviors: causes, impacts, and solutions

Steven H. Appelbaum (John Molson School of Business, Concordia University, Montreal, Quebec, Canada)

- The average cost of a corporate data breach increased 15 percent in the last year to $3.5 million.
- Security incidents caused downtime of more than 8 hours for 31% of impacted organizations.
- The involvement of business continuity management reduced the cost of data breach by an average of almost $9 per record.
- 54% report that electronic crimes by outsiders were more costly or damaging
- Each lost or stolen record containing sensitive and confidential information costs a consolidated average of $145.10
- North America saw a 7% decrease in financial loss attributed to security events.
- Companies in the U.S. and Germany paid the most at $246 and $215 per compromised record, respectively.
- Financial service
- The cost of a security breach leapt 282% in healthcare.

Source: Thanks to David Shephard (netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/) who pulled together these statistics from the 2015 Cyberthreat Defense Report (CyberEdge https://cyber-edge.com/)

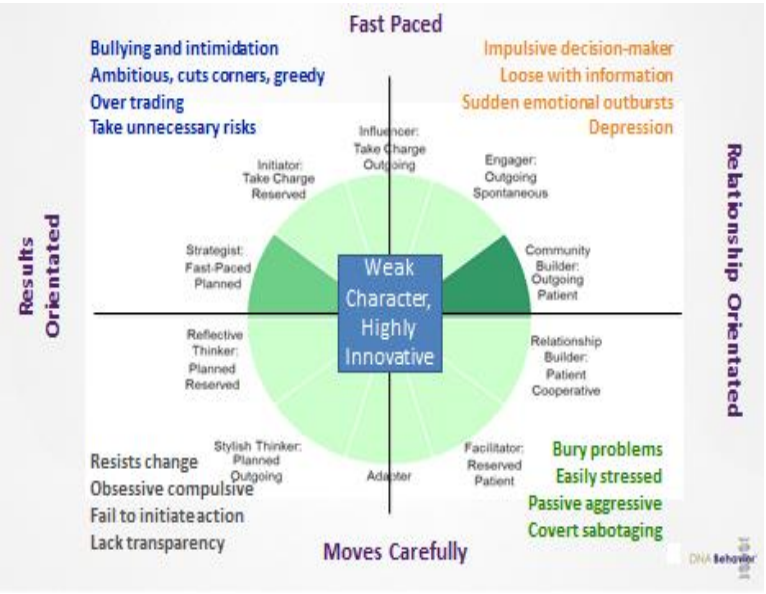
DNA Behavior®

Key motivators for malicious insider breaches

Whilst there will be many triggers that cause people to commit malicious insider action, there is likely to be a causal experience that affects motivation and leads to rogue behavior. This behavior can be revealed and monitored. It is likely to surface as a result of environmental causes such as unaddressed discontent; personality clashes, unchecked bullying, significant organizational change and predator intervention towards a disgruntled employee.

Motivation:-

- Financial gain
- Ideology
- Desire for recognition
- Divided loyalties
- Revenge
- Adventure/thrill
- Ego/self -image
- Vulnerability to blackmail
- Compulsive or destructive behavior
- Family problems
- Negligence



Where Are We Vulnerable? Which Employee is the "Molotov Cocktail"?

These are wise questions asked of the security consultancies that companies retain to analyze and monitor security. Other than tightening operational security, preventing rogue behavior must begin with the hiring process. The organizational culture which insists on robust measures at this first stage will gain a reputation that counteracts the powerful psychological forces encouraging disgruntled employees to go rogue and make bad decisions.

The use of a validated personality insights discovery process at the hiring stage, and also as a retrofitting exercise throughout the organization, will identify:

- Personalities that change significantly under pressure
- Behaviors that manifest if challenged
- Masked character – what lies below the surface
- Toxic team, supplier and client relationships
- People most likely to manage transactions (for example) inappropriately
- Employees who could intentionally attempt to transact outside approved boundaries when placed under personal hardship

The outcomes will lead to more efficient and effective organizational mapping and provide significant benchmarks. For example:

1. The ability to identify combinations of groups, partnerships and teams that work more effectively together.
2. The environment that causes individuals or groups of people to be potentially toxic to the business.
3. The capability to meet the security standards set under ISO 9001:2015 Risk Based Thinking.

People hired for their talent alone without any consideration of their personality or behavior expose the business. We see fires break out where executives and team leaders drive their people too hard and then wonder why there is a negative reaction and push back from the team. We see scheming between two or more dissatisfied employees, yet fail to foresee the potential consequences from such liaisons.

There is no one factor in isolation that results in the 'Molotov cocktail':

1. **Negative personality traits** – inability to identify a negative combination of traits, biases and emotions that may be triggered
2. **Superficial hiring process** – failure to use adequate behavioral and assumptive interviewing to get below the surface to character, integrity and performance issues
3. **Weak organizational design** – lack of balance in the structure of employee relationships and reporting lines
4. **Inadequate internal controls** – weak monitoring processes to detect unusual patterns of behavior
5. **Personality mix -**Teaming personalities without any understanding of how they work or communicate together

6. **The impact of change on employees** -people who have had no intention of causing harm to the business when employed react to changes and latent destructive behaviors and mindsets surface.

7. **Overused employees** - once passive and loyal become volatile, often allowing themselves to be manipulated by others who are stronger and seeking to do harm.

8. **Pattern of significant change from past behavior** - especially relating to increased nervousness or anxiety, unexplained depression, hyperactivity, decline in performance or work habits, deterioration of personal hygiene, increased friction in relationships with co-workers, isolating oneself by rejecting any social interaction

9. **Ignored gossip** - about a colleague's train wreck of a private life and offer no intervention; these scenarios could result in disrupting or disabling business operations and yet they are predictable!

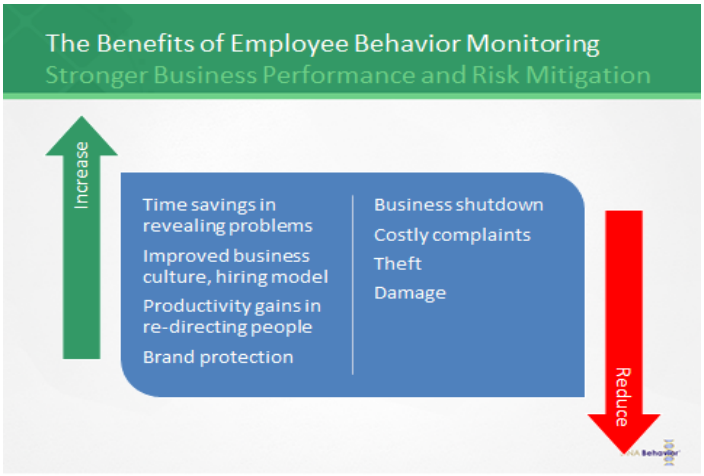
But within these broad headings the most dangerous personality traits are:

- Weak character – flawed decision-making under pressure
- Innovative – bright mind which turns into curious and devious thinking
- Ambitious – desire for success leading to cutting corners
- Secretive – working under cover and not revealing key information

The Benefits of Employee Behavior Monitoring

Organizations regulate internet use, or website visits by their workforce, through two regular ways: by restricting access to particular links, and by monitoring employee actions (***Alampay & Hechanova, 2010***).

Protecting business strength and mitigating risk is more than monitoring IT behavior, though this does have a place. The rogue within is far more likely to reveal his/herself at times of pressure either within the organization or as a result of outside influences.



Knowing in advance the degree to which individuals might react negatively under certain circumstances and whether or not this places the business under threat increases operational safety considerably.

How the Business DNA Solutions Enhance Operational Risk Management

DNA Behavior is an international people insights firm offering the world's only all-in-one behavioral analytics platform for reliably discovering all dimensions of employee, client and contractor personalities.

We provide businesses with a single technology platform which delivers practical and scalable behavioral intelligence solutions to "Know, Engage and Grow" your people.

From hiring to matching talents to roles; from teams to leaders; from advisors to clients/customers, our human capital solutions offer significant insight into personalities and the degree to which, under pressure, these personalities might surface to place the organization at risk.

Revealing the likely maverick behaviors that place the business in potential jeopardy we provide the board and management with scientifically tested suites of personality insights, with reasoning why there may be security or compliance risks with specific employees, why identifying negative outlier behavior before it is triggered can provide added protection, and the online tools and strategies for monitoring and addressing these insider-threats on a real time basis.

Predict Employee Behavior - Options for Evaluation

The typical standard hiring/screening process doesn't reveal all aspects of a person and looks at past actions through background checks. The key issue is what could the employee potentially do in the future? The threat of employees going rogue at some future time is significant enough that organizations are turning to behavioral analytics which are able, not only to detect insider security threats as they happen, but, to predict them well ahead of time. The introduction of behavioral science increases the accuracy of the hire exponentially.

Forced-Choice Scoring Enhances Long-Term Predictability - Quicker and 91% Reliable

Very often the natural DNA behavior sits below the surface; it is not seen because it is masked by the more dynamic (situational) learned behaviors that are shaped by the person's life experiences, education and values. The Forced Choice Scoring personality inventory used in the Business DNA® Discovery Process is designed as a highly validated psychometric model to provide insight into the instincts, needs, motivations and temperament of an individual (often reflected as the "will do" aspect)

as evidenced in their natural behaviors related to life, work place, business and financial decision making.

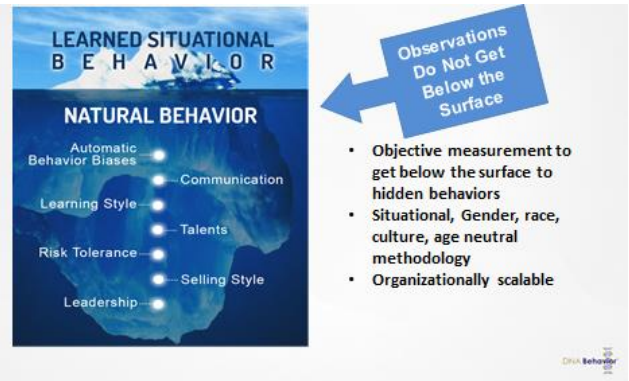
The Business DNA Discovery Process uses non-situational phrases that consistently measure specific ingrained behaviors and automatic biases over time. Its outputs are easy to understand and the assessment is very difficult to "game" and delivers 91% reliability.

Revealing behavior that lies below the surface and what trigger points introduced into the work environment could turn strengths that were seen as positives at the hiring level into struggles leading to rogue behavior.

The Signals and Red Flags

The business needs to set up monitoring procedures which identify the signals in the noise that trigger rogue behavior. The signals can be categorized as: (i) emotional drivers, (ii) unusual activity, and (iii) organizational structure as summarized below:

There are many other indicators that should send up red flags. See Appendix A.



The outcome of external analysis results in the need for significant investment into tightening up hiring processes, together with the introduction of software platforms designed to oversee 'key-strokes' in the business. Historically, little or no attention is paid to the personalities of those engaged to conduct business.

> **Human behavior is 93% predictable**. Source: Northeastern University Professor of Physics Albert-László Barabási
>
> http://www.northeastern.edu/news/stories/2010/02/network_science.html

Companies that engage only in IT based security analytics are more likely to miss the point that at the center of any potential threat is a human being. Identifying the triggers, emotions and environmental indicators that cause negative behavior toward the company can halt potential significant security and compliance risks to the business.

DNA Behavior®

Personality Traits Categorized

Using scientifically tested suites of personality insights such as Business DNA, can provide management with the reasoning why there may be security or compliance risks with specific employees, why identifying negative outlier behavior before it is triggered can provide added protection, and the online tools and strategies for monitoring and addressing these insider-threats on a real time basis.

Some practical examples would be:

1. An example: a shrewd and ambitious sales person, well able to achieve targets is placed under pressure to sell a new service. They see others selling faster than them and begin to make promises to clients that cannot be supported by the business. When this doesn't work and their sales figures slip followed by a reduced bonus, they begin to talk to competitors about providing insider information…..their secretive and ambitious style turns to poor decision making and the rogue is born – placing the business in danger.

2. A leading global motor vehicle manufacturer who has always been considered the reliable face of the motor industry faces potential losses from which they may never recover because an ambitious and heavy handed executive in the organization made decisions to cut corners on product testing, failed to share their decisions, endeavored to increase market share by distorting information about the performance of their cars in key areas.

Matching and Mapping

Dysfunction within teams leads to devastation and creates territory within which rogue behavior and threats to the business can be formed. Malcolm Gladwell records in his book *Outliers*, *"*No one—not rock stars, not professional athletes, not software billionaires, and not even geniuses—ever makes it alone." Team and the behaviors cultivated within them need to be managed.

With the use of the Business DNA online personality insights, the business will have the behavioral data for dynamically matching its employees in teams, its sales teams with customers or clients, and leaders to departments or teams to avoid potential conflict and volatile behavior. Further, this data will provide a deeper understanding of the environmental changes that could promote outlier behavior resulting in negative actions towards the business.

DNA Behavior®

Toxic behavior is more likely to occur in large work teams rather than small ones, probably because large teams are harder to manage closely. The report found strong evidence that employees exposed to toxic behavior are more likely to engage in toxic behavior themselves. Therefore, toxic employees have the capacity to poison the entire organization. Cornerstone OnDemand Survey http://workplaceinfo.com.au/hr-management/performance-management/analysis/identify-toxic-employees-before-damage-is-done#.V9txtFt97Z4

The unique DNA Behavior approach can: score, filter, prioritize employee personality insights through:

- **Mapping:** to identify toxic employee relationships in and with other teams, suppliers and clients
- **Matching:** using algorithms dynamically overlay outlier behaviors with critical roles, transaction activity, communication flows, events to predict rogue employees
- **Knowing:** by deploying Business DNA Discovery Process with all employees to identify outlier behavioral traits
- **Taking action by:**
    - Incorporating into Big Data
    - Sending security alerts
    - Monitoring
    - Re-assigning
    - Developing

When Strengths Become Struggles

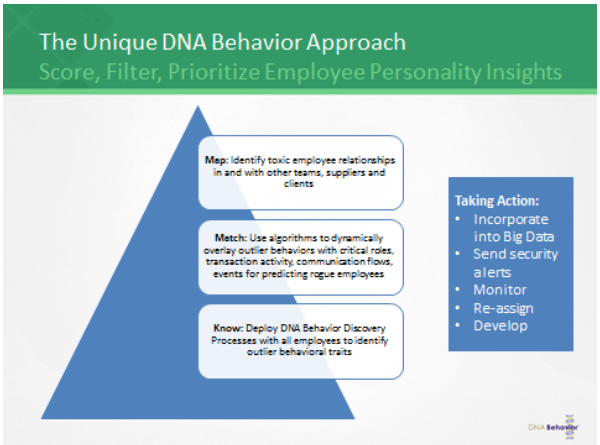
Environmental factors can cause strengths to become struggles and can trigger behaviors that lead to disruptive and destructive behavior.

Changes to patterns of behavior need to be investigated if the rogue is to be uncovered. Some examples are:

- A person required to work away from a team environment shows behavior that moves from being naturally reserved to secretive. They withdraw from mixing socially and when asked about work issues, deliver cagey responses. This could suggest, at best, covering up mistakes and at worst, manipulating data for profit.
- A person that is ambitious, achievement-oriented and commanding faces an equally competitive colleague; their responses become too forceful. They look for ways to cut corners so they don't lose their edge, or perceived status. The stronger the strength, the greater the danger of taking it too far. Rogue behavior begins as they make impulsive decisions and jeopardize the business.
- A person hired for their innovation and creativity becomes frustrated when the business fails to get new offerings to market before rival organizations do. As they see customers leave and go to rivals the employee turns their frustration into rogue behavior by 'selling' their innovative creative ideas to the highest bidder.

The Benefits of Employee Behavior Monitoring

Having the data to hand which reveals potential personality weaknesses, probable responses to a precipitating crisis, and highlights when intervention is required, are significant tools to have. Remembering that no one trait by itself is typically enough to trigger unwanted behavior. Rather, it is a collection of conditions and character issues which cause an otherwise reliable person to intentionally compromise security. Having the ability to monitor such behavior in real time offers significant protection to any business.



Overall, the business will learn how to identify potentially rogue employees and toxic relationships of employees, advisors, teams, suppliers and clients where their behaviors can be predicted to cause increased security risks. Research shows that the following problems are caused by human behavior:

1. Combinations of human behavioral factor outliers and external environmental factors (e.g. financial difficulty, family issues etc.) trigger emotions causing negative behavior toward the company

2. Combinations of employees with similar or different styles working in a high risk environment can cause internal control issues

3. The operational and compliance monitoring processes in certain environments are not equipped to identify and manage the impact of emotionally triggered behavior

The Signals Appendix A

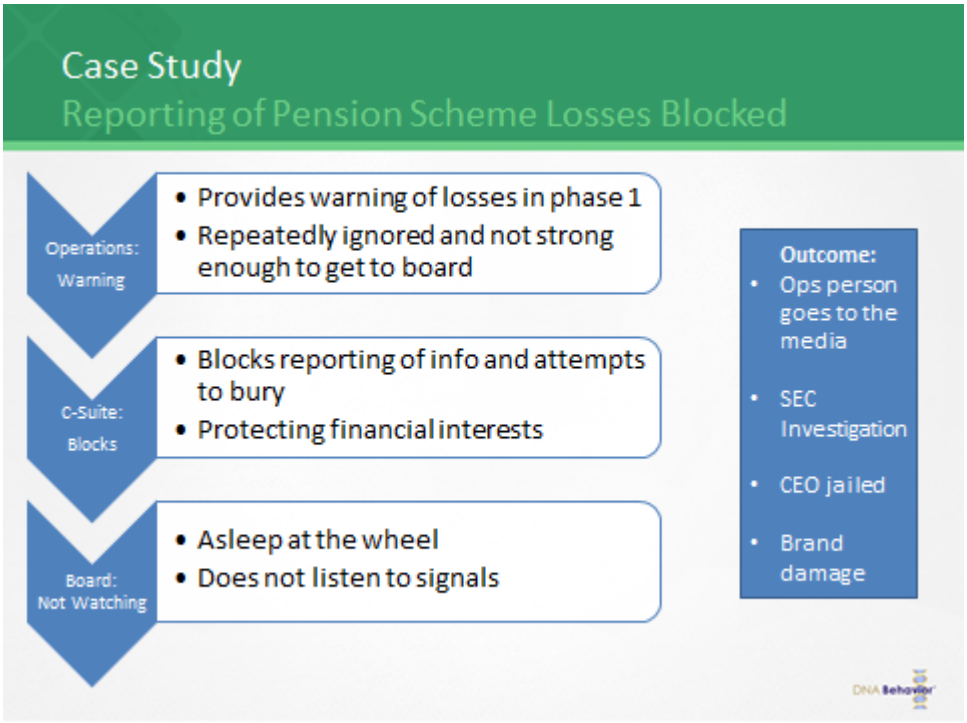
Under pressure what appears to be stable behavior can change with the strengths being strongly and blindly over-used and therefore becoming struggles. If these struggles are not managed they become rogue thereby exposing themselves in some of the following ways:

- Actual or threatened use of force or violence
- Pattern of disregard for rules and regulations
- Spouse or child abuse or neglect
- Attempts to enlist others in illegal or questionable activity
- Drug abuse
- Expression of bizarre thoughts, perceptions, or expectations
- Pattern of lying and deception of co-workers or supervisors
- Talk of or attempt to harm oneself
- Writing bad checks
- Failure to make child support payments
- New team leader
- Different work procedures
- Pay freeze
- Market downturn placing employees vulnerable to lay-offs
- Persistent argumentative or insulting behavior toward colleagues

- Significant changes from past behavior.
- Decline in performance
- Extreme reclusive behavior
- Loss of confidence, nervousness and anxiousness
- Becoming secretive and reclusive.
- Appearing intoxicated at work
- Sleeping at the desk
- Unexplained, repeated absences on Monday or Friday

Case Study 1

Reporting of Pension Scheme Losses Blocked



The CEO failed to inform the Board of the full extent of the pension scheme's losses in one of its portfolios. Even when senior management continued to highlight the problems, the CEO did not bring the losses to the Board's attention. The CEO, normally a strong, decisive, but fair leader, suddenly becomes intimidating, unapproachable and hostile to the suggestions of his management team. No one challenged this change in personality.

In addition the Board, also subjected to the CEO's forceful behavior, failed to adequately ask questions and look into the detail of how well the pension scheme was actually performing, therefore failing in their fiduciary duties.

This deliberate effort by the CEO to conceal information was compounded by the fact that the management team, who could see the danger, were not sufficiently in control of operations to challenge the CEO.

The pension scheme was now financially exposed, and at risk. In frustration and concern from a fiduciary perspective of being ignored, a senior member of the executive team makes an anonymous call to the media. The headlines were very ugly as the cover up and fraud was revealed. What followed damaged the business significantly.

The potential for rogue behavior began at the hiring process for the CEO. The twice divorced candidate was hired. No alarm bells rang at the financial cost of the CEO supporting two families. Unknown to his management team the CEO was facing his third marital breakdown and was trying to protect his position and annual bonus in light of a further financial settlement.

Case Study 2
High risk trading of Accounts –Losing the Money

David and Paul had always managed their own investments. Over their 30-plus year's partnership, they made most of their investment decisions together using each other as a sounding board. They stayed in stocks and took a long term view. They considered themselves safe investors.

David and Paul decided that with the growth of their interior design business it was time to seek professional help and find a financial advisor.

They completed their research and settled for a financial advisor known to mutual friends. Even at the first meeting David and Paul felt intimidated by the over confidence of the advisor. He dominated the conversation with assurances of how he could increase their wealth. He brushed off their comments about low risk tolerance. They found themselves acquiescing to anything the advisor said.

The alarm bells rang loud and clear when just a short time later the adviser immediately redeemed a material portion of their mutual funds, so the money could be shifted to his choice of funds. David and Paul anxiously watched as their investments fluctuated up and down in a seemly endless churning of investment opportunities. Exchanges of worried phone calls to their advisor were met with confident assurances there would be upside in the long term.

Alarmed at the significant losses David and Paul fired the advisor. They realized how domineering the advisor had been and how submissive they had been.

DNA Behavior®

Contact DNA Behavior International

Our Operational Risk Management Team consists of individuals with extensive experience, knowledge and skills that will be able to help your organization identify and address critical security risks which are caused by employee behavior. Our team would be pleased to discuss your needs and can be contacted at:

DNA Behavior® International

5901-A Peachtree Dunwoody Rd

Suite 375

Atlanta, GA 30328

USA
Telephone: +1-770-274-0311

Fax: +1-770-274-0315

www.dnabehavior.com