livingsecurity

TECHNICAL WHITEPAPER

Human Risk Index (HRI)

The Quantification of Human Risk

Introduction

This technical whitepaper is written for security professionals to understand a new approach to quantifying human risk using the Bayesian (or "belief") Network, a method of statistical inference that captures assumptions and gathers information from continuous inputs of hundreds of predefined criteria based on the data integrations set up by your organization. This method is the building principle behind Living Security's Human Risk Index (HRI), a proprietary, patent pending model that consistently and effectively sorts users and groups into five distinct levels of risk.

This whitepaper breaks down the technical elements to provide security teams the information on how the model assesses risk, aggregates the data, and surfaces the data in an easy to understand method.

The HRI is the quantification component of a Human Risk Management (HRM) approach, a foundational and groundbreaking strategy disrupting the cybersecurity industry[1]. HRM is used to identify, respond to, and report on human-initiated risk within an organization. HRM represents the convergence of granular understanding of human behavior that impacts cyber risk in a negative or positive way and prioritizing actions taken to quantifiably reduce risk overtime.

[1] forrester.com

Key Takeaways

1. Understand why security leaders struggle to consistently and effectively track, measure, and reduce human risk.

2. Discover how Living Security's Human Risk Index empowers you to make informed decisions and drive change in the organization.

3. Learn why the Bayesian Network model and machine learning are the foundation for the Human Risk Index.

4. Identify how to utilize the Human Risk Index to deliver ROI, reduce human risk through action plans, and create a more vigilant security culture.

Learn more about Human Risk Management.

Challenge: Inadequate or Disparate Human Risk Quantification Capabilities

As cyberattacks continue to escalate, especially focused on people, it has become clear that existing efforts like Security Awareness & Training (SA&T) have been inadequate to reduce workforce risk. With the move to incorporate a Human Risk Management approach into an organization's security programs, CISOs need a way to quantify human risk similar to how security risk assessments identify gaps in security controls. Often security leaders rely on technology, such as email, endpoint, web, and identity and access tools to identify risk associated with end users. Or they rely on User and Entity Behavior Analytic (UEBA) tools that gather and process network event insights to detect the use of compromised credentials, lateral movement, and other malicious behavior. Individual tools or behaviors tracked through a UEBA often create alert fatigue and lack the ability to capture an aggregate view of data to determine true pockets of risk or vigilance in your workforce.

At this point, CISOs either dedicate an analyst to configure and run expensive UEBA tools, attempt to manually build their own analysis from individual tools using spreadsheets, which is both inefficient and often outdated as soon as it's complete, or they do nothing at all.

The requirement for CISOs to quantify human risk in real-time in order to track trends and take appropriate actions to address the risk posed by employees before an incident happens is a real challenge. Aggregating data, correlating it, and deriving actionable insights can be a tremendous and heavy lift for teams of any size to change behaviors, and change risk. Consistently and effectively communicating human risk resilience of an organization, group, or individual, requires the use of existing user behavior data from multiple existing security tools fed into an intelligent algorithm to deliver actionable human risk scores.

> **...it is important to progress from the traditional security awareness model to that of using behavioral science to change the habits that lead to attack path breaking actions.**
>
> verizon✓
>
> *Verizon 2021 Data Breach Investigations Report*

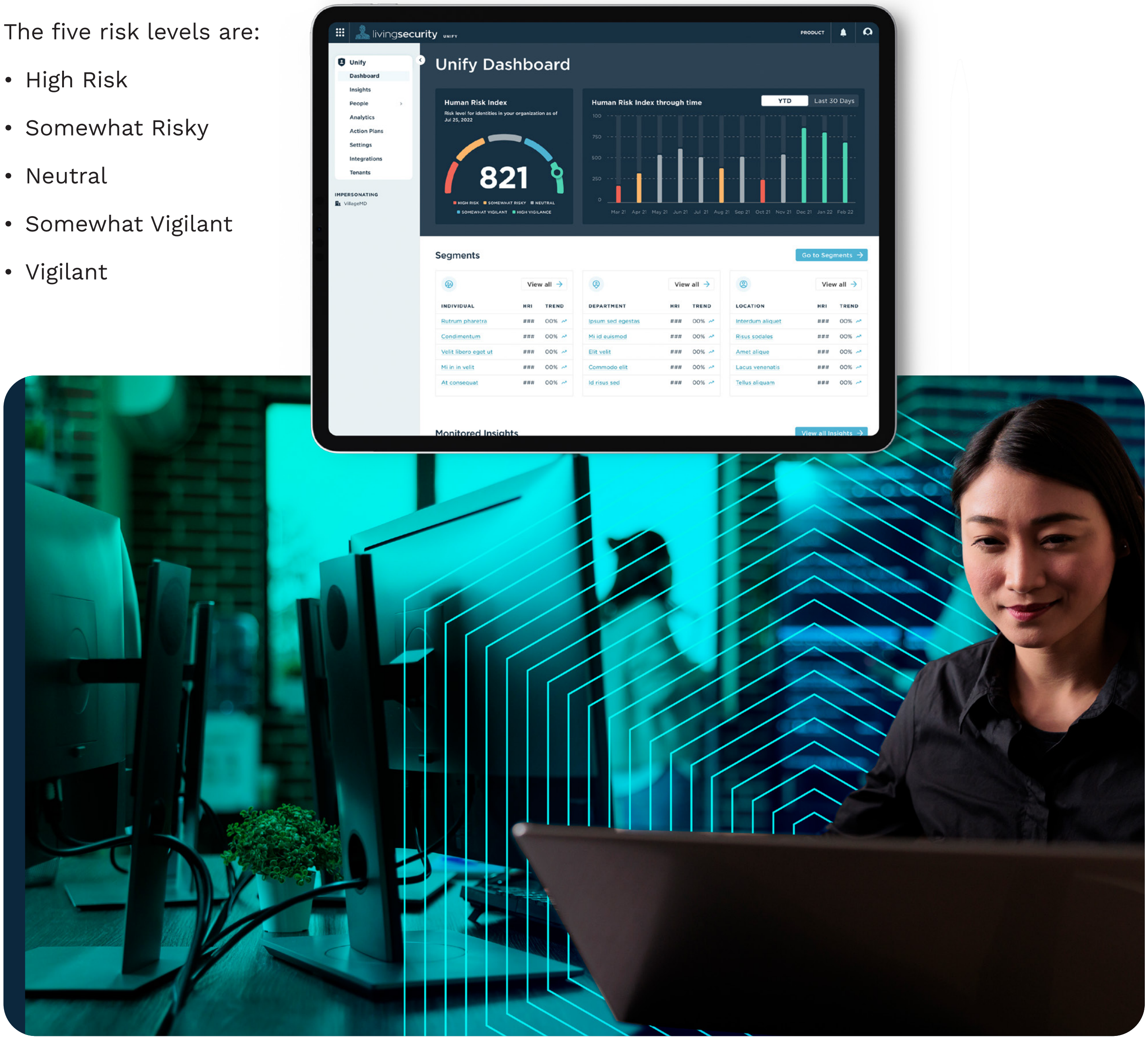
Solution:
Human Risk Index – Effectively Identify, Quantify, and Reduce Risk

The goal of the Human Risk Index (HRI) is to provide a simplified yet highly accurate snapshot of an individual, segment, or organization's risk potential given the presence of behaviors. From risky behaviors such as using incorrect passwords, clicking on phishing links, and working on devices prone to malware, to vigilant ones such as completing training, reporting suspicious emails, and correct use of password managers, each individual's behaviors are reflected on their HRI score.

Using the HRI, CISOs can swiftly and accurately quantify the risk of individuals and groups across an organization into five distinct levels of risk. This is based on the data integrations your organization has set up through Living Security's Unify platform, pulling in hundreds of data points into one easy-to-understand index.

The five risk levels are:

- High Risk
- Somewhat Risky
- Neutral
- Somewhat Vigilant
- Vigilant



INDIVIDUAL	HRI	TREND
Rutrum pharetra	###	00%
Condimentum	###	00%
Velit libero eget ut	###	00%
Mi in in velit	###	00%
At consequat	###	00%

DEPARTMENT	HRI	TREND
Ipsum sed egestas	###	00%
Mi id euismod	###	00%
Elit velit	###	00%
Commodo elit	###	00%
Id risus sed	###	00%

LOCATION	HRI	TREND
Interdum aliquet	###	00%
Risus sodales	###	00%
Amet alique	###	00%
Lacus venenatis	###	00%
Tellus aliquam	###	00%

How the Human Risk Index Model Was Created

The Human Risk Index (HRI) was created by a team of data scientists and is calculated using a Probabilistic Graphical Model (PGM). This approach provides a way of estimating the likelihood and impact of human behaviors toward overall security posture. In other words, from the integrations from your own technology stack into the Living Security Unify platform, data points are then gathered, correlated, and analyzed through the model to determine the HRI score.

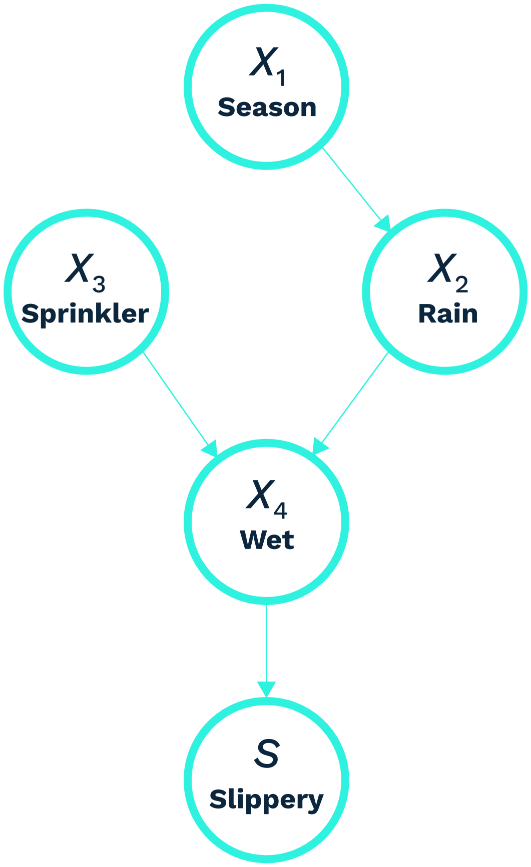
Human Risk Index Algorithm

The HRI uses observed data points from your security tools to estimate the probabilities of higher-order human behaviors. Our team of data scientists has worked to develop a robust and effective algorithm that brings together many different human behavior data points across your existing, siloed technology platforms as well as open-source intelligence (OSINT) data to give a clear picture of human risk exposure.

A Probabilistic Graphical Model seeks to answer the questions:

- Given a certain behavior, what is the probability that something else would occur as a result or connected to that behavior?
- How are different behaviors and outcomes correlated or conditional upon each other?
- Do certain behaviors increase risk, and if so, why and by how much, and in what areas?

HRI specifically uses a Bayesian (or “belief”) Network (BN). BNs codify the joint probability of several variables by organizing them into a network structure that shows which variables have causal relationships with one another. It’s easy to see just how many variables can affect the outcome, and increase the probability of a security incident. Scaling this up to an enterprise process becomes overwhelming. This is why an HRI is made to be a flexible, precise way to infer the dependencies between multiple human risk variables, and how those variables are related to a variety of potential outcomes.

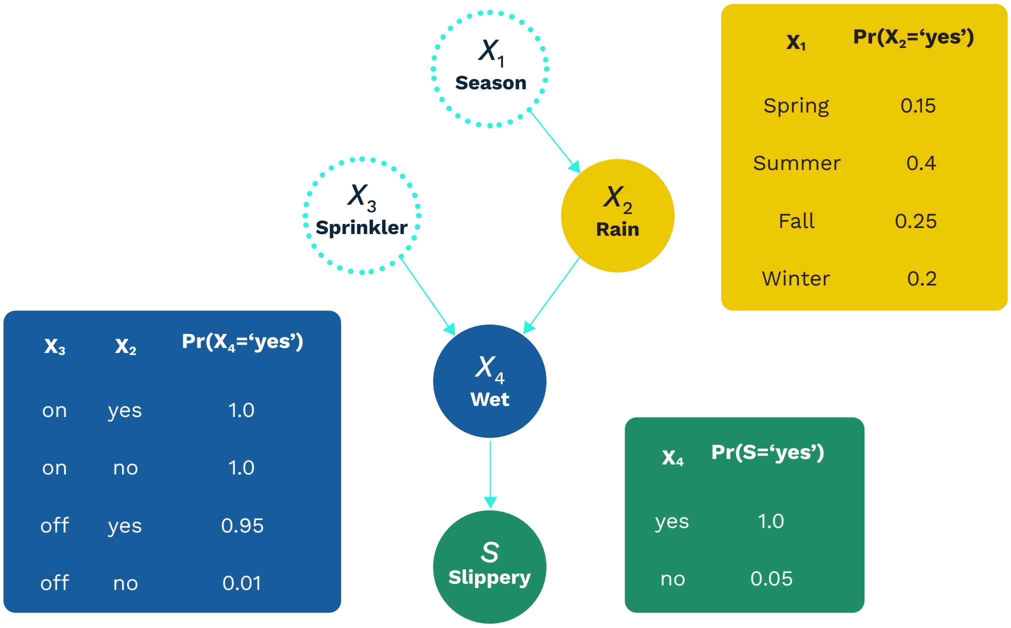


Ex. Bayesian Network

Source: Judea Pearl, Causality: cambridge.org

Cybersecurity is a complex and often enigmatic field where, at the end of the day, CISOs sometimes can't be entirely sure why an incident occurred. It would make everything easier if it were always an "if this, then that" situation. Instead, it's much more convoluted than that, with many more variables at play. Are employees who frequently forget their passwords more or less likely to fall for phishing schemes? Is someone who is vigilant about using their password manager going to be better or worse at spotting and avoiding malware? How would you know?

The advantage of using a BN is that we can look at complex causal relationships to more accurately predict downstream outcome, given a set of known, observable inputs, and one or more layers of inferred variables. This collection of variables is organized into a directed acyclic graph (DAG), where the nodes represent random variables and the edges define conditional dependencies among those variables. In particular, a Causal Bayesian Network (CBN) is one where each directed edge in the DAG represents a causal relationship. The CBN is fully specified by defining a set of states for each variable (e.g., high/low) and identifying its conditional probability table, which declares how incoming nodes coordinate to affect its predicted state.



X_1	Pr(X_2='yes')
Spring	0.15
Summer	0.4
Fall	0.25
Winter	0.2

X_3	X_2	Pr(X_4='yes')
on	yes	1.0
on	no	1.0
off	yes	0.95
off	no	0.01

X_4	Pr(S='yes')
yes	1.0
no	0.05

Ex. Causal Bayesian Network

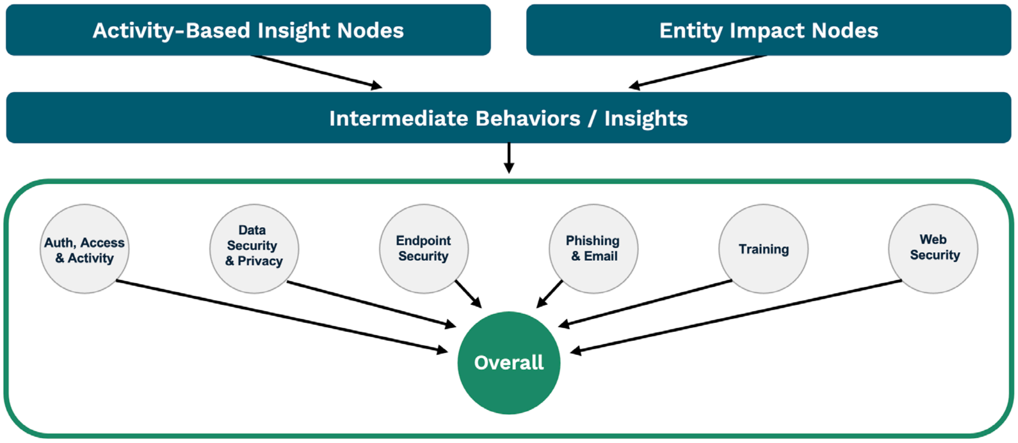
Source: Judea Pearl, Causality: cambridge.org

This provides a visual and interpretable analytic hierarchy of how an employee's underlying activity gets mapped to one or more insights, and ultimately how those insights are combined into a score for a given security category—specifically the likelihood that a user is/is not a risk, given the insights we've derived about them.

We've chosen to use a CBN (as opposed to other types of graphical models) because it's more interpretable than other more generic types of BNs, it's more intuitive for a modeler to build and modify over time, and it's convenient for classification tasks—one can treat predicting an HRI level for individuals as a classification task.

How Behavior Indicators and Impact Modifiers Adjust the Human Risk Index

Unique to Living Security, the Human Risk Index is built to take into account both risky as well as vigilant behaviors, and it can be adjusted based on the impact modifiers specific to that individual. Different individuals in different parts of an organization, or even different groups, can have much more impact on sensitive information, data loss, and other attacks based on the access they have within a company, so this context is important.



Ex. Using Behavior Indicators and Impact Modifiers to Adjust the HRI

Observed Behavioral Indicators

Things that an individual was observed doing at a point in time or over time, each of which can be risky, vigilant, or neutral.

Examples:

- Matt visited a malicious website at a high rate (risky)
- Matt installed the latest OS patches today (vigilant)
- Matt visited 100 websites today (neutral)

Impact Modifiers

Things that are a characteristic of an individual, which has the potential to dampen or amplify the impact their behaviors have on their HRI.

Examples:

- Amanda is a VIP
- Rudra has privileged financial access
- Paul has privileged IT access
- Boris is a tenured employee
- Destiny is a new (untrusted) employee

The ability to not only aggregate risky behaviors, but also to show CISOs where risky behavior most urgently needs to be addressed in an individual or group is something the Unify platform with HRI was built to do. This data-driven approach is flexible, accurate, and customizable to your organization, and it frees CISOs up to tackle real threats before they become major incidents.

VillageMD

> *"Unify allows me to not only focus on which departments are exhibiting the most cyber risk, but it provides me with the data I need to focus on why these behaviors are taking place. For example, 90% of my workforce's risky activities are going to have a legitimate business reason to do what they're doing. Unify Insights helps me have the context needed to discuss the risky behaviors and present the business reasons on why this behavior needs to change and what actions the organization can take to mitigate this risk."*
>
> ***– Dan Walsh, CISO, VillageMD[2]***

[2] VillageMD Case Study

How Utilizing the Human Risk Index Extends Far Beyond the Security Team

Living Security's Human Risk Management platform was built to serve multiple stakeholders' needs, and it all starts with an accurate, quantifiable view of current risk with the Human Risk Index. When sources of risk are aggregated in one easy-to-understand view, CISOs can partner with others across the organization to improve human risk exposure based on measurable, current data, not guesswork or accusations.

Individuals

Individuals want to be able to do their jobs without interruption. They want to understand their specific actions that contribute to increasing or decreasing risk rather than be grouped into the whole company or team to complete generic, one-size-fits-all training. But most security teams lack the ability to determine this level of detail across their organizations until it's too late and an incident has happened and they are investigating. Employees often don't know what it is they're doing that is making them or the organization more vulnerable, but knowing this information and how to improve or better partner with security teams in vulnerable activities that are still necessary for their roles, can lead to empowerment and change in behaviors and improved HRI scores.

Management

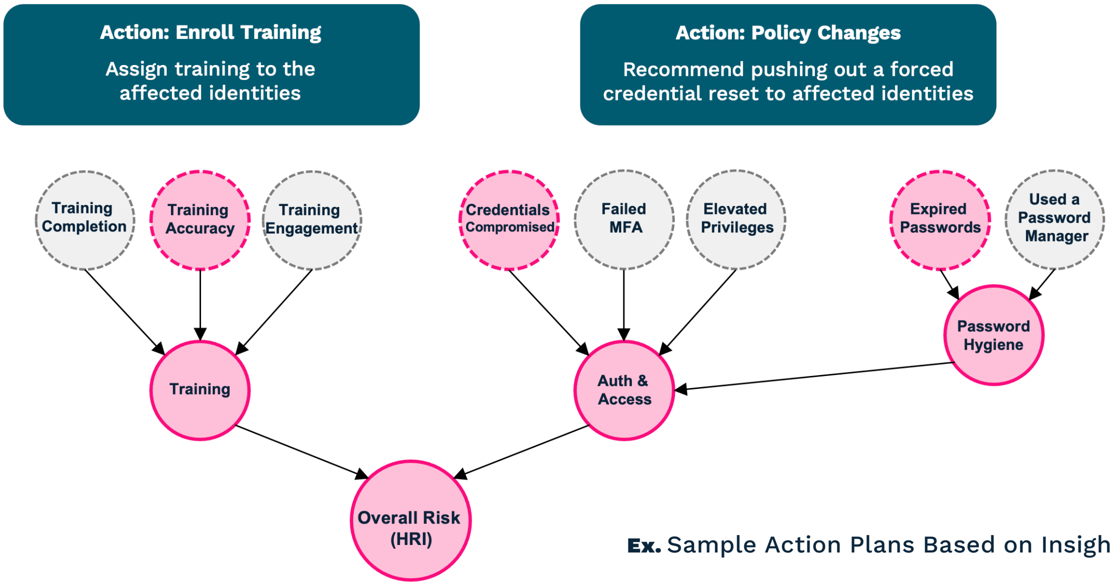
Managers want to know their teams' or team members' HRI scores to encourage improvements and changes in activities as necessary. This access to data can focus their efforts to change behavior through gamification and departmental competition.

Using the Human Risk Index to Reduce Risk and Save Time

The insights that make up the HRI come from the correlated data from your organization's security and other workforce-centric platforms, evaluating hundreds of data points to provide context around specific business risk categories. The HRI model doesn't change by the amount of data captured. However, the more integrations and data points ingested, the more valuable and comprehensive your HRI scores will be across six key risk categories including:

- **Access and Authentication:** Provides insights that decrease the likelihood of account compromise success.
- **Data Security and Privacy:** Decrease the likelihood of IP/data loss by seeing which individuals and groups are riskiest.
- **Endpoint Security:** Decrease the likelihood of ransomware downloads.
- **Phishing and Email:** Identify most targeted users across the email attack landscape, reduce phishing email click rate, reduce the likelihood of business email compromise, and increase user reported phishing emails.
- **Training and Assessments:** Measure the efficacy of your training in a much more detailed manner that goes beyond completion rates and quiz accuracy to show actual behavior changes.
- **Web Security:** Decrease in "drive by downloads", improvement in web browsing behavior, reduction in executable downloads, reduction in malicious files downloaded to user systems, and reduction in browser cookie information.

From the Unify dashboard, admins are able to filter their view by risk category and drill down into specific activities that contribute to the corresponding risk level. This allows them to understand the individuals or groups that fall into which risk categories and why. With this knowledge, action plans can be triggered or operational changes can be made to make a positive impact on the HRI score and even specific behaviors. Ultimately, tracking human risk in a consistent and predetermined manner levels the playing field across the enterprise, helping everyone understand how to reduce their risk exposure to the organization.



Action: Enroll Training

Assign training to the affected identities

Action: Policy Changes

Recommend pushing out a forced credential reset to affected identities

Ex. Sample Action Plans Based on Insights

Conclusion

At Living Security, we believe that the last frontier of cyber risk is the human aspect.

The Human Risk Index, which powers the Human Risk Management platform is an innovative solution in the market today. Living Security combines the Bayesian model with Machine Learning (ML) to remove the time, money, and resources necessary to create such robust and actionable metrics. A predefined human risk criteria that is clear and consistent to measure makes it simple for organizations to track human risk and vigilance from day one.

With Human Risk Index, security leaders can:

- Make informed decisions on how to best prioritize security resources to decrease risk in your organization.
- Have the most current data easily accessible to discuss trends, ROI, and issues with executives and leaders.
- Create efficiencies across the security team with focused efforts on targeted risk areas rather than pulling together data and creating reports that are out of date upon completion or one-size-fits-all approaches to vigilance.

When you know where the risk is, you can manage it to decrease the potential impact of an incident to your organization, leveraging each and every individual to be a part of your security defense.

For more information, contact Living Security

livingsecurity

About Living Security

Living Security's mission is to transform human risk to drive dramatic improvement in human behaviors, organizational security culture, and infosec program effectiveness. With our Human Risk Management platform, Living Security engages each employee with innovative and relevant context and content, while simultaneously providing the ability for leadership to identify, report on, and directly mitigate the risk brought on by human behavior.