



Human Risk Management

MATURITY MODEL

The new approach in changing human behaviors
to protect organizations from cyber threats.

E-Book

INTRODUCTION

Human Risk Management Maturity Model

Technology and Structure Advancement

The modern attack surface has expanded following advancements in digital transformation and the post-pandemic shift to a remote or hybrid workforce, consequently creating more backdoors for adversaries to gain entry. In 2021, there were [31%](#) more cyber attacks than the previous year. Sophisticated cybercriminal activity, alliances, and Ransomware-as-a-Service business models make it more difficult for people to avoid falling victim to their tactics. In fact, more than [82%](#) of all data breaches involve a human element, demonstrating that cybersecurity is no longer just a technical challenge, but a human one as well.

Humans are the Last Frontier of Cybersecurity

Organizations have focused on securing devices, applications, networks, and data, but largely neglected the role of people as a component of security—concentrating instead on check-the-box compliance training that has a discernible influence on reducing risk. In a recent report, Gartner found that 93% of employees performing certain unsecure actions in the workplace already knew their behavior increased risk to their organization. The question facing CISOs today is how to stop employees from engaging in this type of risky behavior. They know they need a comprehensive approach to manage human risk; however, CISOs are unsure how to gain board and company-wide buy-in, correlate existing data across disparate technologies to understand human risk, and provides reports to change in the organization.

”

“What is overwhelming our security organizations is the risky human behaviors and daily human failures, not the big, notable incidents. These smaller missteps are happening millions of times a day and if you want to lower the onerous demand on your security team, you need to focus on Human Risk Management.”

- Dan Walsh, CISO, VillageMD



It's Time for a Paradigm Shift

Compliance is a great first step to managing human behavior. But there's little to no evidence that training people specifically for compliance purposes reduces risk. Organizations should be doing both. Changing the behaviors of employees is the ultimate goal to improve security posture—not just training engagement or completion. This requires a new approach and an evolution from today's security awareness methodology to a Human Risk Management approach.

Human Risk Management Approach Drives Change

Human Risk Management represents a transformation in how enterprises should identify, respond to, and report on human-initiated risk within their organization.

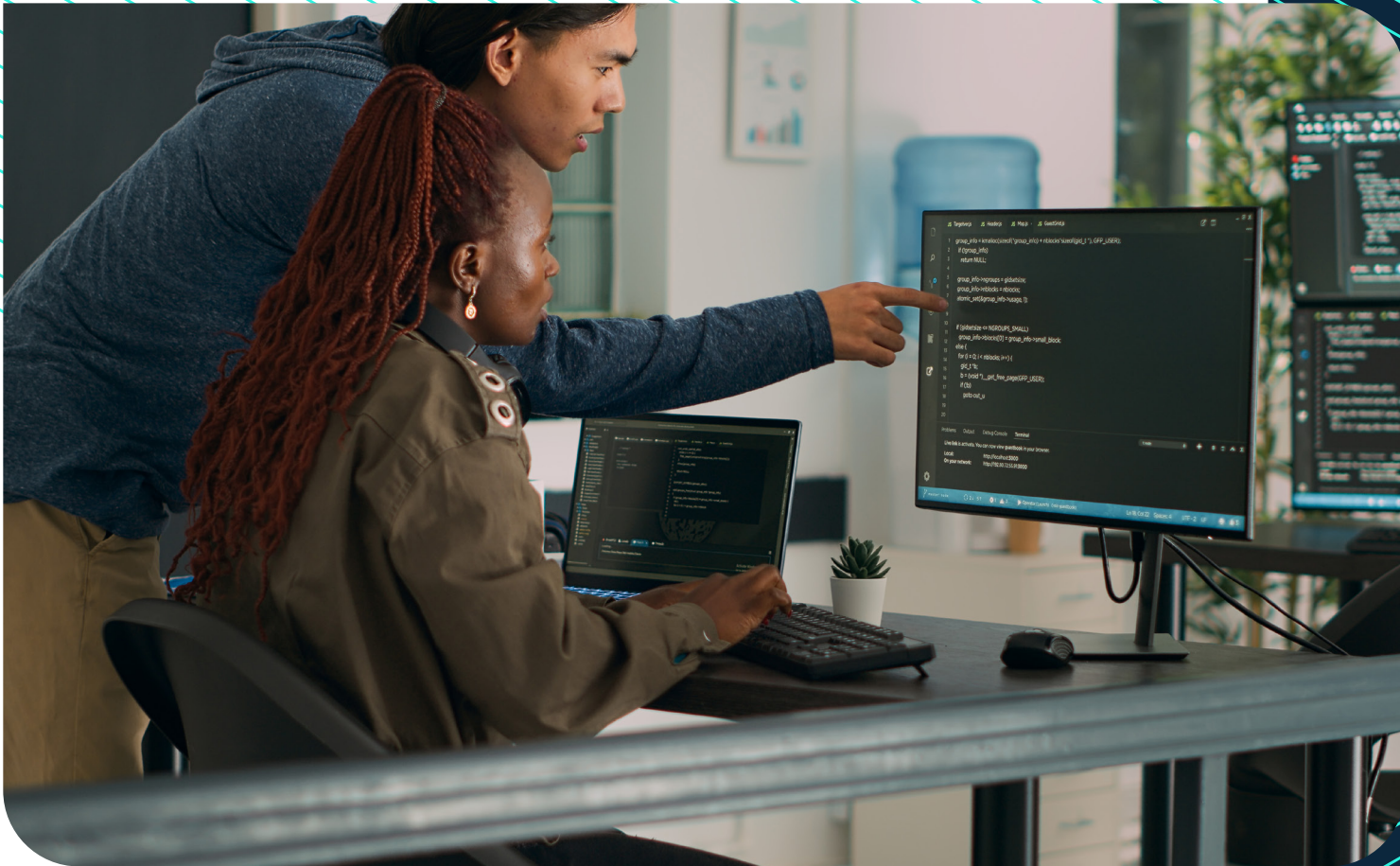
Human Risk Management is the result of incorporating three overarching trends seen in the security and risk management space:

1. the realization that compliance does not equate to security,
2. the shift from point-in-time snapshots and assessments to continuous reporting and improvement, and
3. the breakdown of siloes, leading to a convergence of technology, data, and applications working together to deliver better results.

A mature Human Risk Management program gives security teams the insights and tools they need to identify key human risks before they escalate into a security event or an incident. It provides users with personalized guidance precisely when needed, and delivers relevant content to build a strong security culture with measurable impact. And by quantifying human risk in all areas of the business, policies are continuously improved.

How to Mature a Program

Compliance is a great first step to managing human behavior. But there's little to no evidence that training people specifically for compliance purposes reduces risk. Organizations should be doing both. Changing the behaviors of employees is the ultimate goal to improve security posture—not just training engagement or completion. This requires a new approach and a evolution from today's security awareness methodology to a Human Risk Management approach.



Maturity Model Overview

The Human Risk Management Maturity Model has been developed in collaboration with cybersecurity industry thought leaders and practitioners. This model provides security teams guidance on building stronger cyber defenses and boosting resilience. When executed well, human behaviors will improve reducing business risk, and allow the security team to become a true business partner to the rest of the organization. Additionally employees will feel empowered, and cultural change will take place, ultimately leading to a more secure world.

How to Use This Model






The Maturity Model is divided into three categories: Culture, Technology, and Process. Within each category are key components that formulate a Human Risk Management program. Each component is measured at its own maturity stage. As you assess your position, you gain a matrix of results to help you prioritize next actions.



Human Risk Management Maturity Model

Categories & Components Defined

Culture

Culture	Workforce Engagement	Mandatory	Remediatory	Incentivized	Buy in	Ownership
	Endorsement	Direct team only	Limited stakeholders & siloed employees	Siloed leadership & some employees	Leadership & broad employees (i.e., security champions)	Company-wide & external stakeholders
	Security Organization	Security reports to IT (buried organization structure), small team, little funding, and tool budget	Security is its own business unite, but continues to educate C-level and board on separation of security & IT, battling for funding and resources. Program budget	Data driven security initiatives funded & Supported with the CISO reporting to C-Suite & board with regularly defined responsibilities with KPIs	Fully funded & supported security organization, with the CISO included in executive level conversations	CISO and/or security diligence is included in business decisions, influencing perception by external stakeholders
		 Initial	 Managed	 Defined	 Optimized	 Innovating

Workforce Engagement

The Workforce Engagement component is the cultural objective describing the underlying drivers of a program focused on human risk.

Initial Stage: Engagement is mandate-driven and aligns with meeting compliance requirements en masse. This is often the stated goal for most security awareness and training programs; however, it is only the beginning for Human Risk Management programs.

Managed Stage: As programs mature, workforce engagement expands to targeted efforts focused on specific risks. For example, a user is enrolled in training after a failed phishing simulation assessment.

While this remedial-driven program has expanded beyond annual compliance requirements and often delivers improved, personalized results for each employee, it lacks a strong sense of individualized ownership of an employee’s impact to the security of their organization.

Defined Stage: In this phase, engagement is incentive-based, offered by the security team, so users start to take the lead in their own training to “win,” either through acknowledgement (champions programs and leaderboards) or rewards such as swag or paid time off (PTO). These incentives provide the catalyst for personal motivation.

Optimized Stage: Evangelists arise throughout the organization, personally motivated to improve cyber hygiene. Workforce engagement is driven by security champions, who become advocates for security initiatives and understand the importance of strong cyber hygiene. Business leaders prioritize cyber-risk conversations, bring awareness to the risks specific to their department or line of business, and even incorporate human risk metrics as part of their performance goals or team objectives.

Innovating Stage: Increased individualized ownership of security by end users who are invested in the cause, both professionally and personally, is solidified. Individuals clearly understand the relationship between their actions and the impact on security, and because of this, they attain a greater sense of ownership at work and at home. Programs that get to this stage typically have operationalized Human Risk Management, using data, processes, and/or technology, to truly change human behaviors at scale.

Endorsement

The Endorsement component measures the breadth of stakeholders who are actively involved in the strategy and support of a company’s overall Human Risk Management program.

Initial Stage: Typically one dedicated individual in the organization is solely responsible for the program. This person often feels like an “island”—the only one who cares about driving behavioral change. They were brought in to ensure compliance and to build a training program, but the lack of organization-wide alignment typically means they have minimal budget, tools, or data to effectively drive change.

Managed and Defined Stage: As the program matures, the individual responsible for the program starts to find advocates in the organization through relationship-building. For example, the program owner enlists marketing or communication teams to help with messaging or branding. Influence will grow from here and foster more leadership support;

however, it's often siloed, not widely coordinated. Similar to the Workforce Engagement component, some end users become champions.

Optimized Stage: Broader leadership endorsement enables wider alignment across the employee base. A key indicator of this coordination-at-scale is when human risk metrics start to become standardized so that they are sharable, repeatable, statistically valid, and used to help focus on the most impactful opportunities. From here, organizations begin to incorporate human risk metrics into tools such as security scorecards, reporting dashboards, embedded security analytics, or used as feedback in performance reviews. These use cases signal top-down leadership support and engagement emphasizing the importance and impact of the program.

Innovating Stage: Security leaders regularly report on human risk programs and related metrics to executives and the board of directors. Often there is a desire to influence external stakeholders. Security leaders may help shape public policy, regulations, or industry standards. In addition, human risk programs may be publicized along with broader cybersecurity programs to build shareholder confidence and brand value.

Security Organization

The Security Organization component evaluates how the broader security program is organized, funded, and prioritized throughout the business. A Human Risk Management program with strong business alignment requires a more mature security organization to gain buy-in and support from leadership and the broader employee base. A simple way to assess this component is for the business to consider whether the security function is seen as a cost center or as a strategic partner.

Initial Stage: Security is typically buried within the IT organization of the company. The head of the security (more often an IT or Security Director rather than a dedicated CISO) has minimal engagement across the C-suite or board and is brought in solely to ensure regulatory compliance. The program is typically underfunded, and security leadership gets “scrappy” to do the basics with their small or non-existent teams.

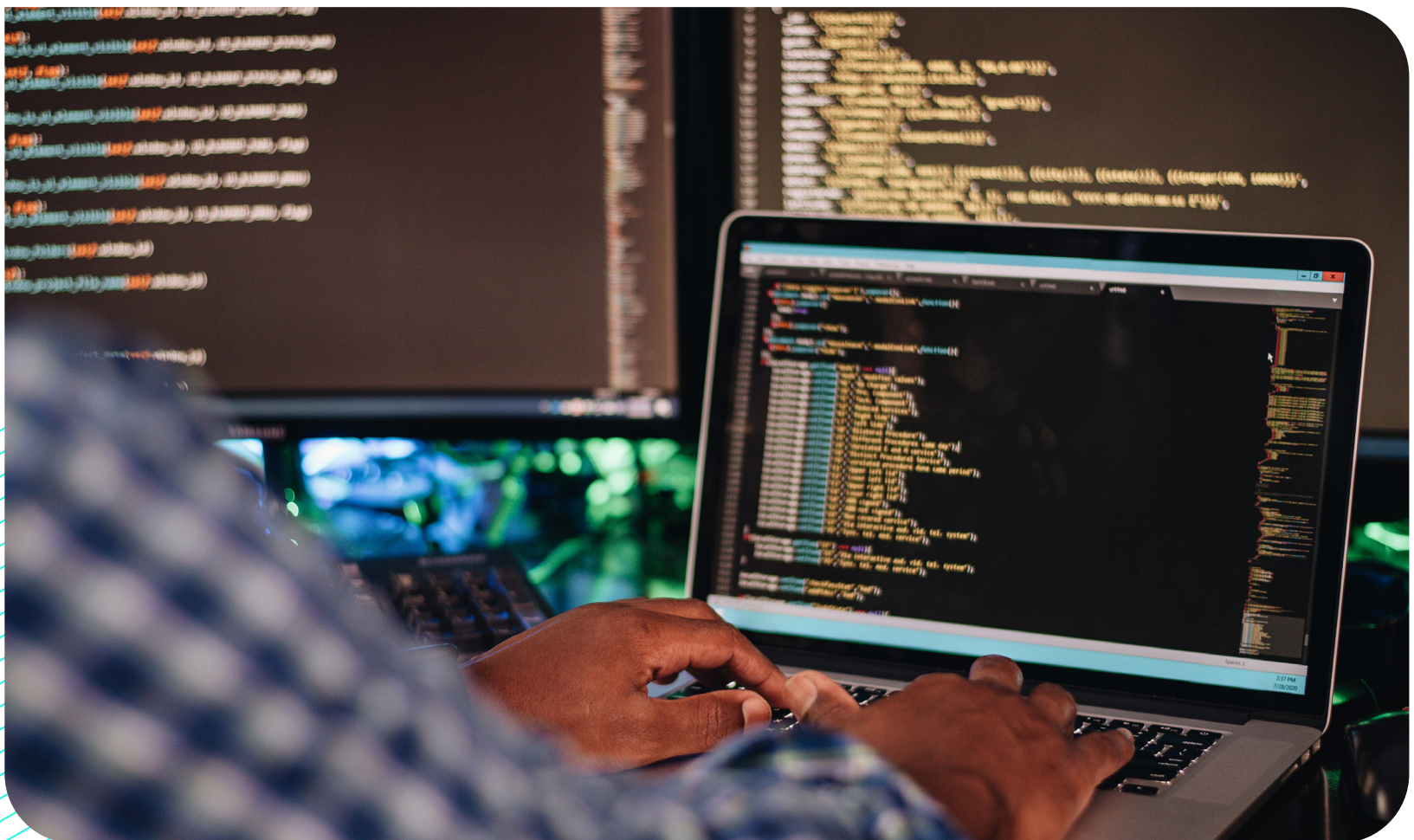
Managed and Defined Stage: An organization will likely have a dedicated CISO that leads a well-structured security program with varied levels of

Categories & Components Defined






influence throughout different business functions. The CISO has visibility across the business, a team with defined responsibilities and regularly reported performance metrics, and regularly engages the executive team and board.

Optimized Stage: Security becomes more strongly embedded in business conversations and decisions. These include proactive third-party risk assessments and a strong influence during the product and/or service development process. The security organization is viewed as a strategic partner within the organization. In fact, the security team often influences merger and acquisition costs given their analysis of risk within the target company because they know if they don't, they must “clean up” after the fact.

Innovating Stage: CISOs often take a role of external influence. Common in highly regulated industries like financial services and healthcare, CISOs meet with regulators and influence policy decisions. In some cases, there is an external-facing CISO role, with a Deputy CISO or other title that performs the internal day-to-day management of the security organization.



Technology

Technology	Tools	Content & LMS, phishing, Small tools budget	Manual spreadsheets for tracking with a small tool budget	Automated spreadsheets, Purpose built training platform	Dashboards that track and report on events, behaviors, risk & context. Including a budget to support a platform	Utilizes an AI tool that delivers predictive risk & response based on benchmarks and proven success Platform budget
	Integrations	Simple CSV upload, Email User management	Automated user management, Phishing & Training integration for remediation only	Reactive to events with manual ecosystem integrations	Automated APIs, proactive information flow and awareness specific integrations	Use of full ecosystem API integrations and predictive modeling
		 Initial	 Managed	 Defined	 Optimized	 Innovating

Tools

The Tools component focuses on the technology systems used by an organization.

Initial Stage: Most organizations have minimal budget for tools. Security program content is often deployed through an internal Learning Management System (LMS), versus a purpose-built security awareness and training platform. Content may be the same year over year, produced in-house or from a vendor. Organizations often use pre-packaged computer-based training that’s included with other compliance programs, despite the suboptimal employee experience. Phishing simulation programs might start at this stage through the use of open-source options or inclusion in a “compliance” bundle offered through vendors.

Managed Stage: As organizations mature in the Tools component, they discover that siloed data points, such as phishing simulation click-rates, aren’t enough to make security training and awareness decisions, so they look for more data from their existing tools. Spreadsheet tracking with some light automation is indicative of a maturing program where activity counts to drive context for behavior change. Commonly, a purpose-built training platform is deployed and provides risk scoring around content effectiveness and allows for targeted campaigns based on segmentation by roles, activity scores, or training efficacy.

Defined and Optimized Stage: Organizations look to automated dashboards that track and report on events, behaviors, and risk with additional context such as tenure, elevated permissions, and susceptibility. This allows for targeted risk-based guidance, interventions, and policy changes that adjust IT security controls based on user behavior.

The Optimized Stage uses tools that deliver nudging or guidance while an employee performs an action. These products produce reporting that show organizational human risk scores, metrics on behavior, and trends over time which are relevant to executive and board-level decision-making.

Innovating Stage: This phase includes the application of machine learning, artificial intelligence, and predictive modeling to automate Human Risk Management. Technology helps identify areas of risk and apply preventive or corrective actions on a continuous basis, with minimal administrative input. These platforms deliver automated controls and personalized training, balancing privacy and security, as well as the business' risk tolerance. Programs in this stage will deliver internal and external benchmarking and use learnings across deployments to recommend configurations and interventions based on proven data.

Integrations

The Integrations component measures the scope of data and tools working together to support the Human Risk Management program, and how integrated the program is with the rest of an organization's technology stack.

Initial Stage: Cybersecurity tools are siloed from the rest of the organization's technology stack. If platforms or products exist at this stage, users are managed through CSV upload, active directory, or other integrations.

Managed Stage: This phase has increased automation, such as consequently enrolling users who show susceptibility to phishing simulation campaigns into training programs.

Defined Stage: Events or activities are integrated into campaign planning or dashboards through spreadsheets and CSV files. This is the start of an “integrated” program.

Optimized Stage: The Human Risk Management program begins integrating with tools outside the scope of traditional security awareness programs. A more holistic picture of human risk is created by collating contextually relevant data from other security tools throughout the organization to use for insight modeling. Security leaders provide risk insights by connecting APIs into their platforms that ingest data on behaviors, user access levels to systems, tenure, threat intelligence, and other OSINT data points.

Innovating Stage: Data flows bi-directionally between a Human Risk Management platform and existing systems to automate control settings, policies, and updating other systems such as Governance Risk and Compliance (GRC), Cyber Risk Quantification, Insider Risk, or Incident Response dashboards. This is when the human factor becomes fully integrated into the broader security landscape and people, process, and technology can function together to create a strong defense.



What is a Human Risk Management platform?

A Human Risk Management platform quantifies, prioritizes, and measures human initiated risks by ingesting, aggregating, and correlating data from your existing security solutions. This end-to-end platform provides security leaders the visibility to manage human behavior induced cyber risk with targeted risk-based action plans, and the ability to analyze and report on trends over time.

Process

Process	Functional Structure	Security is a shared responsibility. Security training is owned by HR, Compliance, or IT	Dedicated security organization & headcount. Security director leads initiatives. Reports through IT and budget is an IT line item	Dedicated organization & team, CISO driven initiatives & budget. Works closely with IT, Risk & some business leaders	CISO driven organization with alignment to executives across functions. Budget to fund key initiatives.	CISO is evangelist internally and externally for Human Risk Management initiatives. Budget adjusts as data based case predicts needs
	Program	Reactive one size fits all compliance-based, annual training, phishing simulations	Reactive, continuous training	Role-based training based on risk scores & types may be optional	Proactive, data driven, and targeted interventions based on risk.	Predictive, risk-based, adaptive and individualized interventions. An ongoing feedback to teams and employees on progress and improvement areas
	Metrics	Compliance check box	Single metric driving decisions (ie. Phishing click rate)	Awareness Program decisions driven by multiple metrics. Policy decisions	Security Program level - driving business decisions/ value Impacting outcomes	Predictive, risk-based, adaptive, Metrics influencing outcomes and business decisions ie: M&A, project staffing like R&D projects, etc.
		 Initial	 Managed	 Defined	 Optimized	 Innovating

Functional Structure

The Functional Structure component revolves around the human risk program itself. Similar to the Security Organization component, this looks at how the program is set up, where it exists in the organizational structure, dedicated resources, responsibility, and funding.

Initial Stage: Awareness and training is a shared responsibility and may exist outside of the security organization with Compliance, IT, Human Resources, or Legal.

Managed Stage: A dedicated full-time headcount to human risk that reports up through IT or Security, which is a typical shift from a traditional structure.

Defined Stage: The program and team work cross-functionally with IT, risk management, or other business leaders, which stems from CISO-driven support and budget that strengthens as the program becomes optimized.

Optimized Stage: The program includes metrics and tools that have an impact across the business, greatly improving the value of the program. This allows for promotions across the Human Risk Management team and senior leadership roles to drive strategy for the program. As budget and perception grow, more specified roles emerge across the team, from data and analytics to culture specialists and others.

Innovating Stage: Budget is driven by the needs of the program to deliver results that align to business objectives and cross-departmentally. The CISO's alignment and evangelism of the program ensure that the value proposition and ROI is visible across the organization, garnering respect and funding.

Program

The Program component incorporates many of the categories already covered but looks tactically at the deliverables to the employee base and where it exists on the continuum of reactive to predictive.

Initial Stage: Maturity is marked by one-size-fits-all training that meets compliance requirements. As maturity grows, the program adds continuous “themes” based on calendar-driven training—typically aligned to their partner's out-of-the-box content roadmap, or if more advanced, a roadmap created internally that is aligned with the business's prioritized risks.

Managed Stage: This phase incorporates training that is more relevant and specific to an individual's job level or role within the organization. Given the alignment and maturity of technology, programs start to deliver training to users based on their “scores” and activities, which are driven by how they perform in training modules and phishing simulation tests. This move to a more personalized approach is a positive sign of maturity and a requirement to move to the next stage of a risk-based program.

Defined Stage: Access to behavioral data is required to provide interventions based on risk.

Optimized Stage: At this phase, the team uses at scale, technology to allow for proactive, targeted interventions based on data.

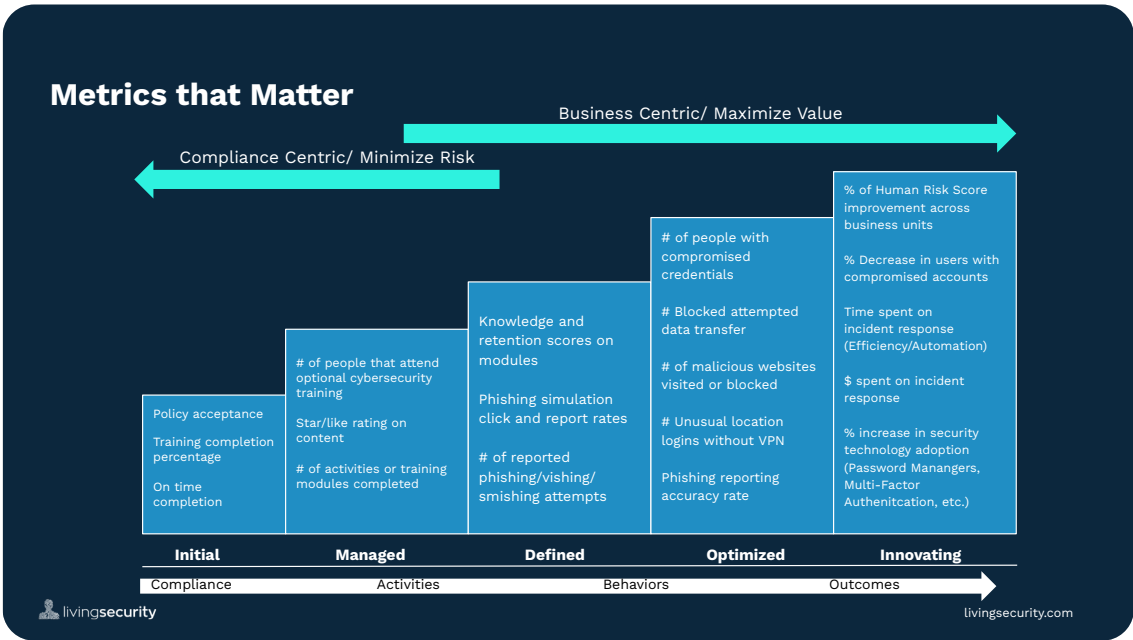
Innovating Stage: Organizations shift from a proactive approach to a predictive approach. Understanding the risk of an individual based on likelihood and impact requires a deeper level of sophistication in modeling and data. At this stage, Human Risk Management programs can take action based on predictive data that a user or group of users are at risk of an incident that would have a large impact. Human Risk Management teams can also provide feedback to employees on their progress in minimizing risk, and information to the business which quantifies the overall impact on risk the Human Risk Management program delivers.

Metrics

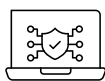
The Metrics component focuses on the evolution of metrics from compliance-centric to business-centric, and the value-based alignment with the rest of the components in the model. These metrics are a tangible output of the work that is being done across culture, process, and engagement areas.

Initial, Managed, and Defined Stage: These stages are typically one-dimensional, focus on engagement and completion rates, and are gathered through manual efforts or captured from individual tools. They follow a “proof-of-work” theme which aligns with compliance requirements.

Optimized and Innovating Stage: In these stages, organizations begin to focus on metrics that are specifically aligned to their security and risk management priorities, often outside the traditional scope of phishing and email security. Metrics become more sophisticated and multidimensional as maturity in the Integrations component grows. At this point, an organization will have made an effort to define, standardize, and prioritize the human risk metrics the program reports on.



Maturity Levels Defined



Initial

Processes are somewhat unpredictable and reactive. At this stage, organizations can complete projects, but the work is mostly ad hoc and undefined.



Managed

Processes are managed on a project level. At this stage, organizations have repeated processes in place that it can follow for success. Some may have rudimentary metrics, but without focus or ability to assess efficacy. Processes are not consistent across the business and there is no notion of their success.



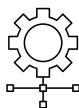
Defined

At this stage, the organization consistently delivers forward-thinking results, being more proactive rather than reactive. Processes are well-defined, acknowledged as standard business processes, and are broken down into more detailed procedures, work instructions and artifacts used to record outputs.



Optimized






At this stage, the organization is more measured and controlled, effectively using data to improve performance and drive decisions. Process management includes a focus on disciplined optimization and continual process improvement. A full team of business analysts measure and assess every aspect of the business for possible issues and improvement opportunities.



Innovating

At this stage, the organization is optimizing and innovating, being agile with a focus on continuous improvement. Organizations use data and predictive models to quickly respond to and anticipate scenarios, either at the project or organizational level.

The Human Risk Management Maturity Model

Culture	Workforce Engagement	Mandatory	Remediatory	Incentivized	Buy in	Ownership
	Endorsement	Direct team only	Limited stakeholders & siloed employees	Siloed leadership & some employees	Leadership & broad employees (i.e., security champions)	Company-wide & external stakeholders
	Security Organization	Security reports to IT (buried organization structure), small team, little funding, and tool budget	Security is its own business unite, but continues to educate C-level and board on separation of security & IT, battling for funding and resources. Program budget	Data driven security initiatives funded & Supported with the CISO reporting to C-Suite & board with regularly defined responsibilities with KPIs	Fully funded & supported security organization, with the CISO included in executive level conversations	CISO and/or security diligence is included in business decisions, influencing perception by external stakeholders
Technology	Tools	Content & LMS, phishing, Small tools budget	Manual spreadsheets for tracking with a small tool budget	Automated spreadsheets, Purpose built training platform	Dashboards that track and report on events, behaviors, risk & context. Including a budget to support a platform	Utilizes an AI tool that delivers predictive risk & response based on benchmarks and proven success Platform budget
	Integrations	Simple CSV upload, Email User management	Automated user management, Phishing & Training integration for remediation only	Reactive to events with manual ecosystem integrations	Automated APIs, proactive information flow and awareness specific integrations	Use of full ecosystem API integrations and predictive modeling
Process	Functional Structure	Security is a shared responsibility. Security training is owned by HR, Compliance, or IT	Dedicated security organization & headcount. Security director leads initiatives. Reports through IT and budget is an IT line item	Dedicated organization & team, CISO driven initiatives & budget. Works closely with IT, Risk & some business leaders	CISO driven organization with alignment to executives across functions. Budget to fund key initiatives.	CISO is evangelist internally and externally for Human Risk Management initiatives. Budget adjusts as data based case predicts needs
	Program	Reactive one size fits all compliance-based, annual training, phishing simulations	Reactive, continuous training	Role-based training based on risk scores & types may be optional	Proactive, data driven, and targeted interventions based on risk.	Predictive, risk-based, adaptive and individualized interventions. An ongoing feedback to teams and employees on progress and improvement areas
	Metrics	Compliance check box	Single metric driving decisions (ie. Phishing click rate)	Awareness Program decisions driven by multiple metrics. Policy decisions	Security Program level - driving business decisions/ value Impacting outcomes	Predictive, risk-based, adaptive, Metrics influencing outcomes and business decisions ie: M&A, project staffing like R&D projects, etc.
		 Initial	 Managed	 Defined	 Optimized	 Innovating

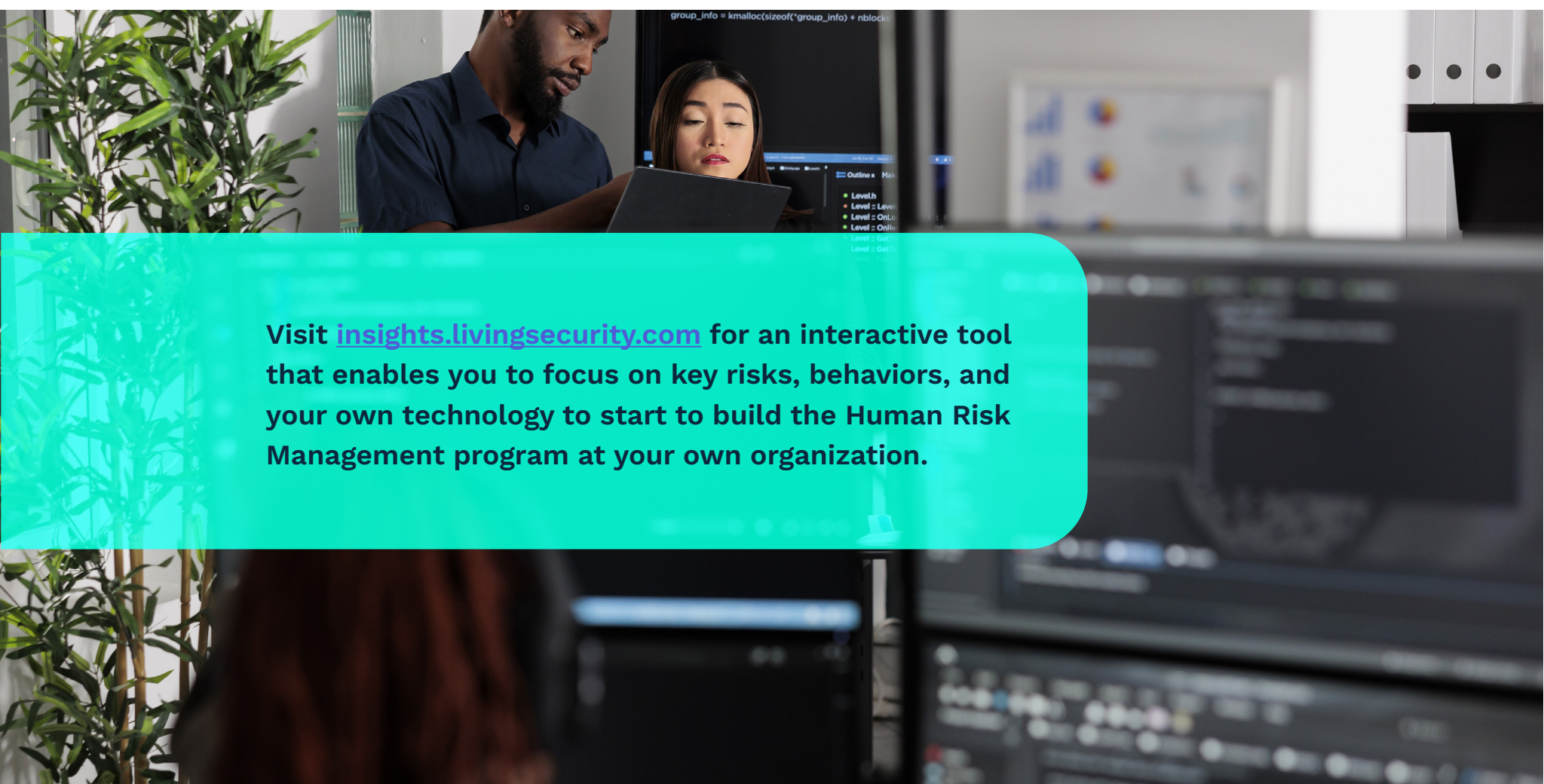
Activities

Behaviors

Outcomes

Conclusion

The Human Risk Management Maturity Model gives security teams guidance to build strong cyber defenses and boost resilience. Improving human behaviors and reducing risk to the business stimulates a positive change in the organization with security becoming a true business partner, empowering employees, and changing the culture. Ultimately, when organizations integrate and mature their Human Risk Management programs, data breaches involving a human element will diminish, making the world a safer place—at home and work.



Visit insights.livingsecurity.com for an interactive tool that enables you to focus on key risks, behaviors, and your own technology to start to build the Human Risk Management program at your own organization.



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.