HRM: *Ask Me Anything*

HRM vs. SAT: What's the Difference?

March 12, 2024 | 11 a.m. ET

Featuring:
Ashley Rose
CEO and Co-Founder
Living Security

Featuring:
Drew Rose
CSO and Co-Founder
Living Security

livingsecurity

We’re seeing the human element increasingly become a bigger part of the risk landscape

This calls for a culture of security

A Shift is Required to Effectively Mitigate Human Risk

Security Awareness

1. Compliance focused
2. Reactive
3. Annual / Predetermined time
4. Computer based training
5. Mandatory buy in only
6. Standalone requirement
7. Executed by any department
8. Checks the box

Human Risk Management

1. Focus on the risk
2. Proactive
3. Just in time, continuous training
4. Targeted action plans
5. Peers understand business risk
6. Part of a larger security strategy
7. Run by the security team
8. Measures your impact

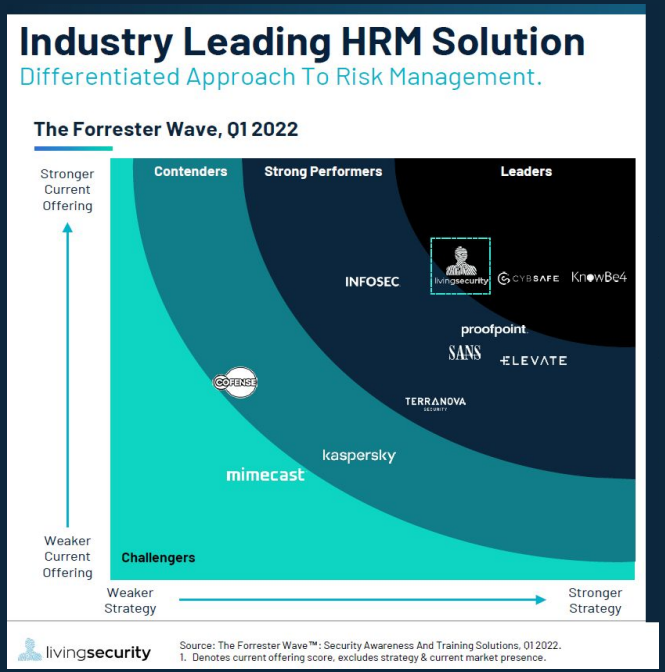
The Future Is Now: Introducing Human Risk Management

"This is not just a name change (aka mutton dressed as lamb)! It is a significant change of mindset, strategy, process, and technology about how we approach an old problem in a new world."

- Forrester

Solutions that manage and reduce cybersecurity risks posed by and to humans through:

1. Detecting and measuring human security behaviors and quantifying the human risk
2. Initiating policy and training interventions based on the human risk
3. Educating and enabling the workforce to protect themselves and their organization against cyberattacks
4. Building a positive security culture



Culture	**Workforce Engagement**	Mandatory	Remediatory	Incentivized	Buy in	Ownership
	Alignment	Direct team only	Limited stakeholders & siloed employees	Siloed leadership & some employees	Leadership & broad employees	Company-wide & External stakeholders
	Security Organization	Silent, Security reports to IT (buried org structure), Small team, little funding. Small tool budget	Security is own org, but continues to educate C-level and Board on separation of security & IT, battling for funding & resources. Program budget	Data driven security initiatives funded & supported, CISO reporting to C-Suite & board regularly defined responsibilities with KPIs	Fully funded & supported security org, CISO included in executive level conversations	CISO/ security diligence included in business decisions, influencing perception by external stakeholders
Technology	**Tools**	Content & LMS, phishing, Small tools budget	Manual spreadsheets for tracking Small tool budget	Automated spreadsheets, Purpose built training platform	Dashboards that track and report on events, behaviors, risk & context. Platform budget	True AI tool that delivers predictive risk & response based on benchmarks and proven success Platform budget
	Integrations	Simple CSV upload Email User management	Automated user mgmt Phishing & Training integration for remediation only	Event reactive Manual ecosystem integrations	Automated APIs, Proactive information flow Awareness specific integrations	Full ecosystem API integrations Ecosystem aware External Predictive
Process	**Functional Structure**	Security (HRM) is a shared responsibility. Security training is owned by HR, Compliance, or IT	Dedicated org & headcount. Security director leads initiatives. Reports through IT and budget is an IT line item	Dedicated org & team, CISO driven initiatives & budget. Works closely with IT, Risk & some business leaders	CISO driven org with alignment to executives across functions. Budget to fund key initiatives.	CISO is evangelist internally and externally for HRM initiatives. Budget adjusts as data based case predicts needs
	Program	Reactive one size fits all Compliance-based, annual training, phishing simulations	Reactive, continuous training, Theme/calendar-based, CSAM etc.	Training based on risk scores & types Role-based, Optional training	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**

Ask Me Anything