2025

livingsecurity

Human Risk Management Calendar

Your Playbook for Proactive Cybersecurity

Now with **metrics-based** action items!

Glossary

UNIFY INSIGHT FOCUS

Discover a Unify Insight that brings your monthly theme into focus, helping you assess and understand the human risks associated with it.

RECOMMENDED ACTIONS

The recommended actions vary based on your Human Risk Management (HRM) program's maturity, focusing on the most impactful steps for measuring and influencing behavioral change. Even small actions contribute significantly to mitigating and managing human risk.

40+

recommended security actions

RECOMMENDED CONTENT

Our security awareness training content is aligned with the topics your HRM program owners will use to address the risk behaviors and threats most critical to your organization.

50+

unique pieces of HRM content*

CAMPAIGN IN A BOX

We develop blog articles, emails, and chat messages every month to align with our monthly theme. You can share this fresh, witty content with your employees within all of your favorite communication channels. To allow ample preparation time, the Campaign in a Box for each month is distributed in the prior month.

*Available through the Living Security Training Platform

2025 Calendar Overview

JANUARY Data Privacy	**FEBRUARY** Artificial Intelligence	**MARCH** Insider Threat	**APRIL** Hybrid & Remote Work Environments
MAY Authentication & Access	**JUNE** Social Engineering	**JULY** Emerging Threat Preparedness	**AUGUST** Data Loss Prevention
SEPTEMBER Secure Web Browsing	**OCTOBER** Cybersecurity Culture	**NOVEMBER** Phishing	**DECEMBER** Shadow IT

JANUARY | DATA PRIVACY

Identify users with unnecessary access to sensitive data and enforce least-privilege policies.
Increase knowledge of organizational data privacy policies.

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24 Data Privacy Week	25
26	27	28	29	30	31	

MONTHLY CONTENT

Unify Insight Focus

Data Downloaded in Bulk

Recommended Actions

High Value: Automate access restrictions based on data sensitivity and provide real-time updates to maintain data privacy standards

Medium Value: Identify Elevated Access employees that have exhibited Data Downloaded in Bulk and send a reminder of internal policies

Additional Value-Adds:

- Remind recent data downloaders about internal policies for managing sensitive data and complying with acceptable usage standards
- Measure policy site visits for any uptick in reviews
- Review training completion numbers and Human Risk Index trends

Recommended Content

- Security Snaps: Downloading Data in Bulk
- Legacy Code Quick Tips: Privileged Access
- Defensive Design: User Permissions & Access Management

Campaign in a Box Delivery

FEBRUARY | ARTIFICIAL INTELLIGENCE

Use AI to identify and prioritize the greatest human risks, improving your threat management. Educate your workforce on proper AI usage to avoid sensitive data leakage.

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
						1 Change Your Password Day
2	3	4	5	6	7	8
9	10 National Clean Out Your Computer Day	11 Safer Internet Day	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	

MONTHLY CONTENT

Unify Insight Focus

Training Completed - Web Security

Recommended Actions

High Value: Ask for early access to Recommendations Engine in Unify
Medium Value: Develop an internal AI policy or revise previous policy to account for developments in the AI threat landscape
Additional Value-Adds: Schedule training and communications on AI usage and internal policies associated with proper data handling in AI models

Recommended Content

- Legacy Code Quick Tips: AI Regulation & Policy Change
- Legacy Code Quick Tips: AI & Misinformation
- Born Secure Quick Tips: AI Chatbots

Campaign in a Box Delivery

MARCH | INSIDER THREAT

Strengthen defenses against insider threats by identifying and controlling risky behaviors, unusual activity and unauthorized access, reducing the risk of internal data breaches

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
2 HIPAA Breach Notification Day	3	4	5	6	7	1 8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31 World Backup Day					

MONTHLY CONTENT

Unify Insight Focus

IDP Suspicious Activity, Suspicious Data Movement, Data Download in Bulk, Unauthorized Media Detected

Recommended Actions

High Value: Set up a Workflow to identify Elevated Access employees with Suspicious Data Movement. Conduct mandatory reviews and acknowledgment of insider threat policies for identified users.
Medium Value: Identify internally agreed upon indicators of insider risk and create a lens for individuals who align with that criteria. Consider access reviews and meetings with those individuals.
Additional Value-Adds: Conduct educational campaigns to reinforce the importance of compliance with security protocols and staying vigilant within work ecosystems.

Recommended Content

- Security Made Simple: Insider Threat Behavior
- Investigate: Insider Threat
- Security Basics: Insider Threat

Campaign in a Box Delivery

APRIL | HYBRID & REMOTE WORK ENVIRONMENTS

Enhance security posture of hybrid workers by educating and improving access policies of individuals that have flexible working environments

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
		1	2	3	4	5
6	7	8 Identity Management Day	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23 National Email Day	24	25	26
27	28	29	30			

MONTHLY CONTENT

Unify Insight Focus

Unusual Location, Impossible Location, Suspicious IP Address

Recommended Actions

High Value: Adjust access levels of Elevated Access, Executive, or Contractors that have had recent Unusual Location Insights

Medium Value: Require travel policy acknowledgments from employees with Suspicious IP Address detections

Additional Value-Adds: Utilize a Workflow in Unify to automatically deliver cybersecurity travel tips to individuals who are traveling or working remotely

Recommended Content

- Security Made Simple: Travel Security
- Security Made Simple: Wi-Fi
- Security Made Simple: Working from Home

Campaign in a Box Delivery

MAY | AUTHENTICATION & ACCESS

Increase knowledge and adoption of password managers, multi-factor authentication mechanisms, and other credential related best-practices. Identify segments with low MFA or Password Manager usage and develop an intervention plan to increase adoption

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
				1 World Password Day	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

MONTHLY CONTENT

Unify Insight Focus

MFA Adoption, Password Manager Adoption

Recommended Actions

High Value: Automatically invite all employees with low MFA adoption or Password Manager usage to to enroll in the organizations preferred tooling. Measure the impact of adoption and employee HRI scores.

Medium Value: Provide business recommendations for updates and/or procurement of additional tooling or policies to mitigate risk identified by authentication and access related Insights

Additional Value-Adds:

- Baseline the number of employees utilizing optional authentication tools like a password manager, MFA or passwordless functionality
- Strengthen password policies based on Unify's risk Insights.
- Deliver credential improvement training to individuals with frequent login failures

Recommended Content

- Security Made Simple: MFA
- Security Snap Celebrations: MFA
- Cyber Social: MFA

Campaign in a Box Delivery

Bonus- Case Study

Unify Identifies MFA Hygiene risk for Financial Institution

JUNE | SOCIAL ENGINEERING

Ensure your highest priority segments are thoroughly prepared for social engineering risks using metrics other than simulation click rate

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30 Social Media Day					

MONTHLY CONTENT

Unify Insight Focus

Phish Targeted and Clicked, Real Phish Clicked, Repeat Phishing Offenders

Recommended Actions

High Value: Identify business group with highest frequency of real phish clicks, malicious email deliveries, and malicious login attempts. Conduct instructor-led training and run specific phishing simulation to improve readiness for sophisticated attacks

Medium Value: Run enhanced phishing, smishing, or vishing simulations to privileged access individuals and automate remediation training delivery

Additional Value-Add:

- Run positive reinforcement reporting campaigns to communicate the impact of a successfully reported malicious phish
- Spotlight employees with the highest number of malicious phish reported in a company-wide newsletter or town-hall

Recommended Content

- Security Snaps: Phish Clicked
- LS Talk: Threat Landscape & Common Attacks for Executives
- Quick Tip: Phishing

Campaign in a Box Delivery

JULY | EMERGING THREAT PREPAREDNESS

Ensure that your employees have a strong cybersecurity foundation in place to contend with the evolving threat actor landscape

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18 National Dapper Your Data Day	19
20	21	22	23	24	25 System Administrator Appreciation Day	26
27	28	29	30	31		

MONTHLY CONTENT

Unify Insight Focus

Unsafe Browsing Habits, Repeat Phishing Offenders

Recommended Actions

High Value: Assign intervention training and resources for highest risk employees based on the most impactful behaviors measured. These individuals will have shown a risky disposition for social engineering, authentication and access attacks, and web security behaviors.

Medium Value: Promote your most vigilant employees in a newsletter or through direct recognition. These individuals will have demonstrated strong hygiene across both social engineering and credential security.

Additional Value-Add:

- Launch optional training and internal blogs focused on the evolving threat landscape
- Create an opt-in communication network to learn about enhancing cybersecurity posture at home

Recommended Content

- Legacy Code Quick Tips: Deepfake Detection Technique
- Quick Tip: Bluetooth Security
- Legacy Code Quick Tip: Safeword Strategy for Family Security
- Born Secure Quick Tips: QR Code Security

Campaign in a Box Delivery

AUGUST | DATA LOSS PREVENTION

Use Unify Insights to predict and prevent data loss incidents

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 / 31	25	26	27	28	29	30

MONTHLY CONTENT

Unify Insight Focus

Outbound Data Policy Violated, Unauthorized Media Access Detected, Data Loss

Recommended Actions

High Value: Adjust access controls of Elevated Access employees or Contractors with data loss prevention Insights

Medium Value: Identify Recent Hires with high rates of data movement and share resources pertaining to proper data handling

Additional Value-Add:

- Assign policy acknowledgment to individuals with DLP associated Insights
- Provide resources to business segments who handle sensitive data frequently

Recommended Content

- Security Made Simple: Data Classification
- Security Snaps: Deleting Data in Bulk
- Security Made Simple: Why Security Matters

Campaign in a Box Delivery

SEPTEMBER | SECURE WEB BROWSING

Mitigate web-based threats by limiting risky browsing behavior and educate employees on secure browsing tactics

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26 National Compliance Officer Day	27
28	29	30				

MONTHLY CONTENT

Unify Insight Focus

Unsafe Browsing Habits

Recommended Actions

High Value: Identify business segments with high rates of secure web gateway alerts and develop role-specific policies. Certain roles may merit intranet access only or mandatory VPN usage

Medium Value: Reiterate acceptable use policy guidelines to recently hired employees who have high rates of Website Blocked

Additional Value-Add: Assign training about the importance of home internet security and IOT devices

Recommended Content

- Born Secure Quick Tip: Staying Safe Online
- Born Secure Quick Tip: Saving Passwords to Your Browser
- Security Made Simple: Virtual Private Network
- Security Snaps: Safe Surfing on Company Devices

Campaign in a Box Delivery

OCTOBER | CYBERSECURITY CULTURE

Build a proactive security culture that addresses human risk factors

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1 Cybersecurity Awareness Month	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17 Clean Your Virtual Desktop Day	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

MONTHLY CONTENT

Unify Insight Focus

Identify your vigilant employees and highlight their success with an overview of all vigilant behaviors

Recommended Actions

High Value: Distribute Human Risk Index or Behavior Score scorecards to employees

Medium Value: Build a recognition program that highlights your most vigilant employees and their behaviors

Additional Value-Add:

- Deliver a cybersecurity newsletter calling attention to the current state of employee risk and vigilance. Share metrics around employee vigilance, reward top performers, and gamify areas for improvement.
- Run departmental workshops focused on HRI and key insights. Consider gamifying by creating a reward for the segment with the highest HRI

Recommended Content

- Quick Tip: Being a Cybersecurity Leader
- Security Made Simple: Security Culture for People Managers
- Cybersecurity Tonight: Cybersecurity is Part of Your Job

Campaign in a Box Delivery

NOVEMBER | PHISHING

Protect sensitive information by measuring vigilance and improving habits of high-risk users. Identify high-risk employees who are frequently targeted and have fallen for recent simulated phishing attempts, such as clicking links, submitting data, or opening attachments

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17 Int'l Fraud Awareness Week	18	19	20	21	22	23
24	25	26	27	28	29	30 National Computer Security Day

MONTHLY CONTENT

Unify Insight Focus

Phish Targeted and Clicked, Phishing Reporting Adoption, Repeat Phishing Offenders

Recommended Actions

High Value: Identify Elevated Access employees who are repeat clickers. Run offensive security measures to enhance preparedness for phishing attempts

Medium Value: Identify segments with lowest and highest phish reporting over 90 days. Provide resources on proper reporting techniques to lowest group. Promote the frequent reporter segment for continued vigilance

Additional Value-Add: Gamify a reward system for individuals who report malicious phish

Recommended Content

- Cybersecurity Tonight Quick Tip: Themed Phishing
- Defensive Design: Phishing for Technical Employees
- Security Made Simple: Alternative Forms of Phishing

Campaign in a Box Delivery

DECEMBER | SHADOW IT

Detect and control unauthorized applications that bypass security protocols

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

MONTHLY CONTENT

Unify Insight Focus

Unauthorized Media Access Detected

Recommended Actions

High Value: Identify individuals who have violated application download guidelines and require policy acknowledgment for future third-party application registration
Medium Value: Distribute reminders emphasizing the importance of updating browsers and software
Additional Value-Add: Create Workflows for individuals with Unauthorized Media Access Detected reminding employees about proper device controls and media sharing

Recommended Content

- Security Made Simple: Unapproved Software
- Defensive Design: Application Portfolio Management
- Security Basics: Shadow IT

Campaign in a Box Delivery

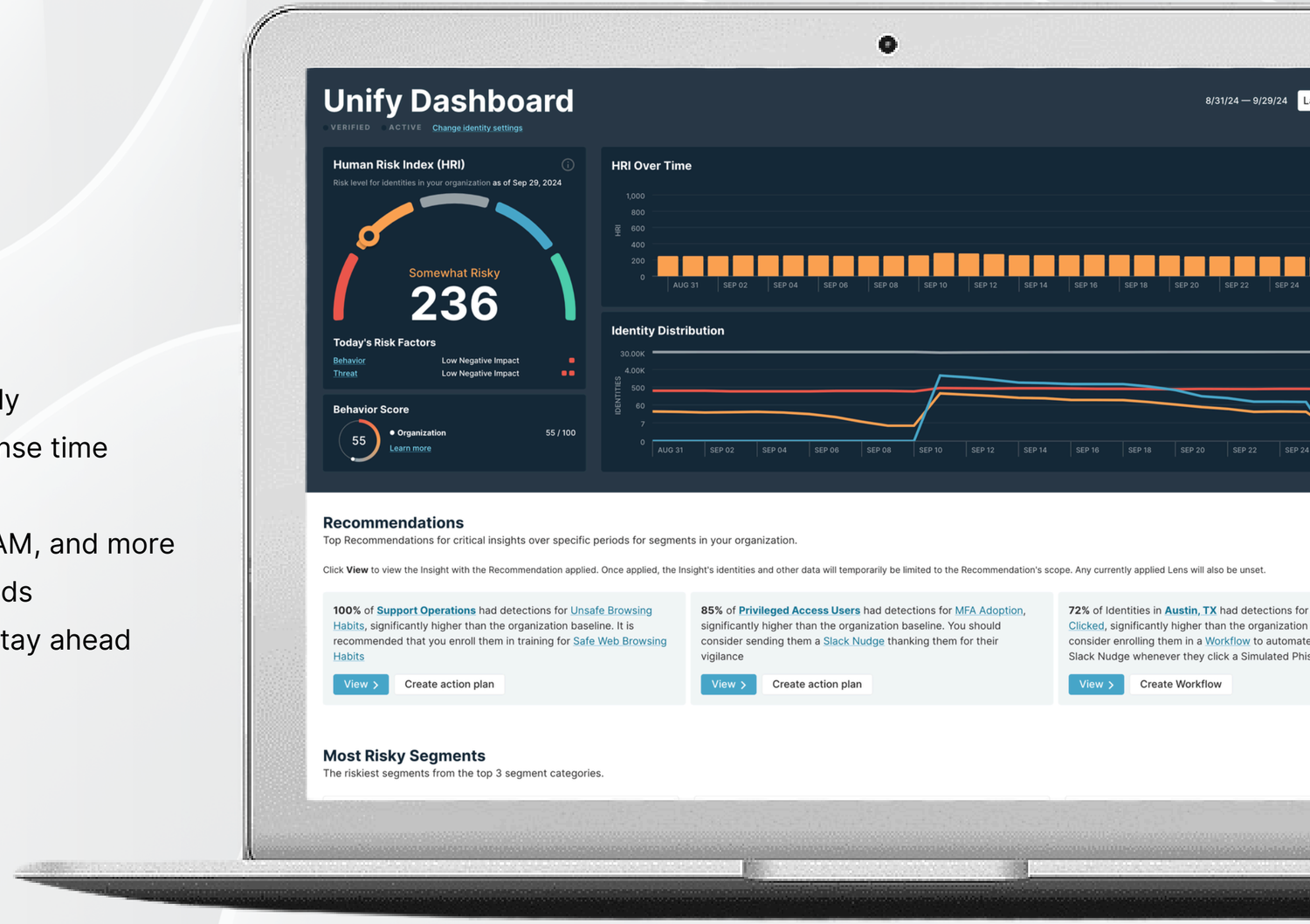
Ready for Proactive Cybersecurity?

Maximize Your 2025 HRM Strategy with Unify

Learn More

Unify's HRM Must-Have Features:

- ***Unified Risk Dashboard:*** Centralizes human risk visibility
- ***Behavioral Risk Scoring:*** Flags high-risk behaviors instantly
- ***Automated Response Workflows:*** Reduces manual response time
- ***Executive Reporting:*** Simplifies board-ready reports
- ***Tool Integrations:*** Connects seamlessly with SIEM, DLP, IAM, and more
- ***Compliance Alignment:*** Maps behaviors to regulatory needs
- ***Threat Intelligence:*** Identifies emerging risks so you can stay ahead



livingsecurity