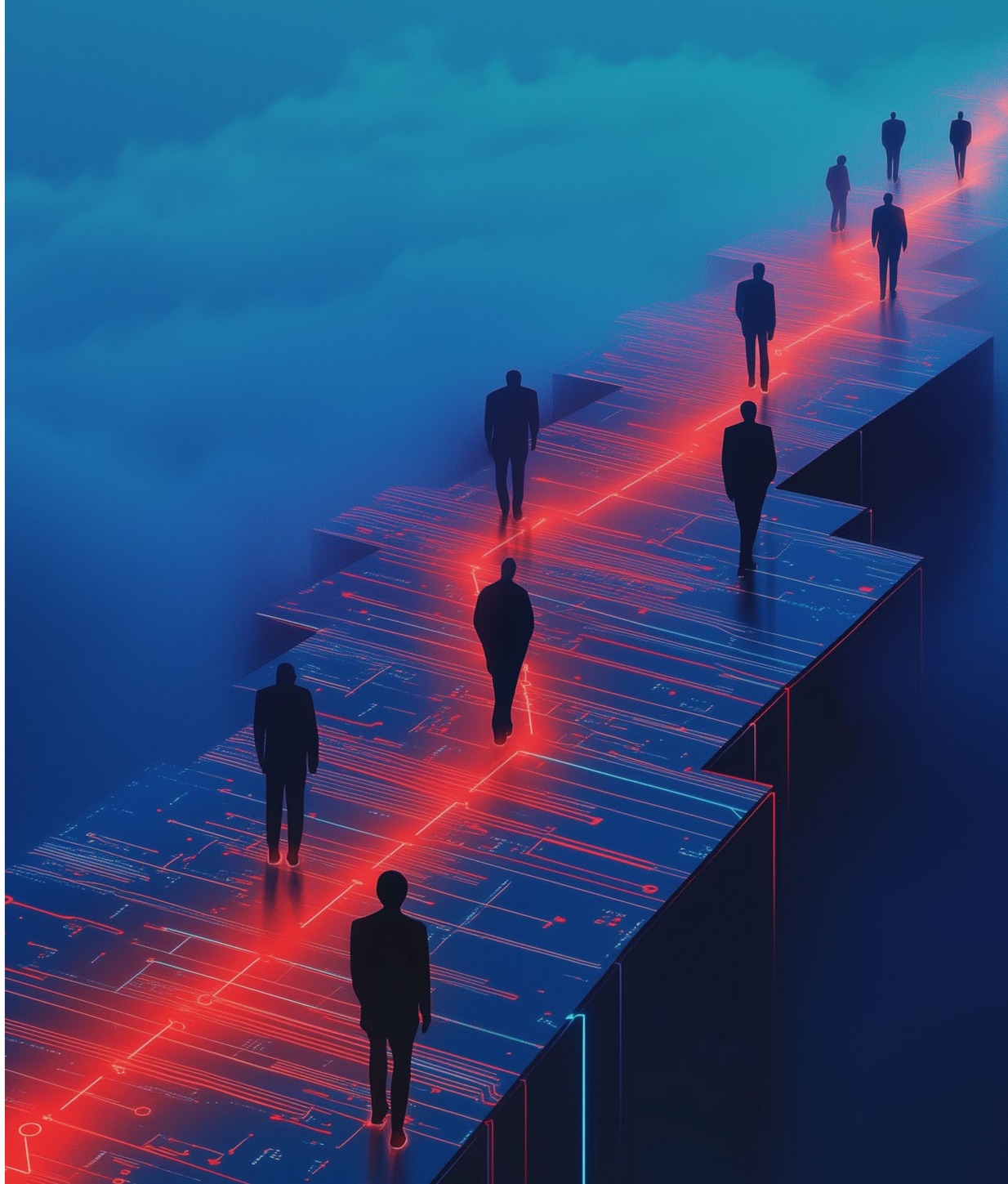
mimecast CDW

Transforming Human Risk: A 90-Day Roadmap to Cyber Resilience

Perspectives on the impact of IT advances on energy optimisation initiatives



INTRODUCTION

The Human Element in Cybersecurity

Your organisation has invested heavily in security infrastructure, yet one simple mistake, a single click on a phishing email, can create significant vulnerabilities. It's a frustrating reality: over 90% of cyber attacks start with email, and just 8% of employees account for 80% of security incidents. Meanwhile, the average cost of an insider breach has climbed to £15 million.

This isn't just a technical challenge, it's a human one.

With hybrid work, cloud-first strategies, and collaboration tools evolving rapidly, employees are making security decisions every day, often without realising the risks. Whether it's clicking a suspicious link, sharing credentials with colleagues, or transferring corporate data to personal accounts, these actions, typically without malicious intent, create substantial vulnerabilities. The challenge is finding a way to reduce risk without disrupting operations.

Security professionals face a dilemma: how to protect collaboration environments whilst empowering users and detecting insider threats, all without adding complexity or impeding productivity.

RETHINKING SECURITY

From Restriction to Enablement

Traditional security strategies focus heavily on restriction, layering policies, enforcing controls, and conducting periodic training. But this approach doesn't address the core issue: security just isn't something people think about every day.

The solution requires a fundamental shift in perspective. Instead of seeing employees as the weakest link, we need to position them as a powerful front line of defence.

The right approach includes:

- Adaptive security that responds to individual behaviour
- Automation that minimises manual intervention
- Contextual awareness that guides employees in real time

Security should work with people, not against them. This ebook lays out a practical, 90-day roadmap to help organisations transform their approach to Human Risk Management, embedding security into everyday workflows seamlessly and effectively.

TIMELINE

The 90-Day Human Risk Management Roadmap

This structured plan breaks security transformation into three manageable phases, each building upon the previous to create lasting resilience:

Days 1-30: Assessment & Visibility

Before you can address human risk, you need to understand where it exists. The first phase focuses on establishing critical visibility into your organisation's risk landscape.

Map Critical Assets & Access

Begin by identifying your most valuable data assets and documenting access permissions. This inventory should encompass proprietary intellectual property, customer information, financial data, and source code repositories. Understanding precisely what requires protection forms the essential groundwork to implement targeted security controls.

Measure Human Risk Patterns

Develop an accurate baseline of your security posture by examining how teams interact with sensitive information in daily operations. Rather than implementing excessive content inspection rules or complex classification schemas, focus on identifying genuine behavioural patterns that expose vulnerabilities. This practical assessment provides actionable insights and reveals specific risk areas requiring attention.

Identify Key Risk Segments

Analyse user behaviour methodically to identify the specific users who represent disproportionate risk exposure. This typically includes personnel with privileged system access, those managing financial transactions, and technical staff with infrastructure access. This precise understanding enables targeted protection without imposing unnecessary restrictions on general operations.

Establish Governance Structure

Develop a structured framework defining clear roles, responsibilities, and evaluation metrics for your human risk management programme. This governance structure should align security initiatives with business outcomes, ensuring that protection mechanisms enhance operational resilience rather than impeding productivity.

TIMELINE

Outcomes by Day 30

By the end of the first 30 days, you'll have built a comprehensive understanding of your organisation's security landscape, providing the essential foundation for targeted improvements. This visibility phase delivers four key outcomes:

A comprehensive inventory of critical data assets with detailed access mapping, revealing exactly what needs protection and who has access.

High-risk user identification, pinpointing the specific individuals and roles requiring enhanced security measures.

Quantifiable risk baseline with clear metrics, allowing you to measure improvement and prioritise initiatives.

Business-aligned governance framework that ensures security initiatives support rather than hinder organisational objectives.

Days 31-60: Implementation & Automation

With visibility established, the second phase focuses on deploying protective measures and automation that strengthen security without adding friction.

Deploy Adaptive Email Protection

Implement AI-powered email security that adjusts protection levels based on individual risk profiles. This approach provides heightened scrutiny for high-risk users whilst minimising disruption for others, stopping phishing attacks and business email compromise attempts before they reach employees.

Secure Collaboration Channels

Extend protection beyond email to collaboration platforms where sensitive information is increasingly shared. This includes monitoring for data exposure in messaging applications, file sharing services, and cloud storage, identifying potential data leakage without blocking legitimate collaboration.

Implement Risk-Based Awareness

Replace generic security training with personalised, contextual education that responds to actual behaviour. When employees engage in risky actions, provide immediate guidance that helps them understand security implications without disrupting their workflow.

Automate Response Workflows

Develop automated response protocols that address common risk scenarios without requiring constant analyst intervention. These workflows should include early warning systems for data exfiltration attempts, unusual access patterns, and potential credential compromise.

TIMELINE

Outcomes by Day 60

By day 60, you'll have implemented key security mechanisms that work seamlessly with your team's daily activities. This implementation phase delivers four practical outcomes:

Adaptive protection across email and collaboration platforms, adjusting security levels based on individual risk profiles.

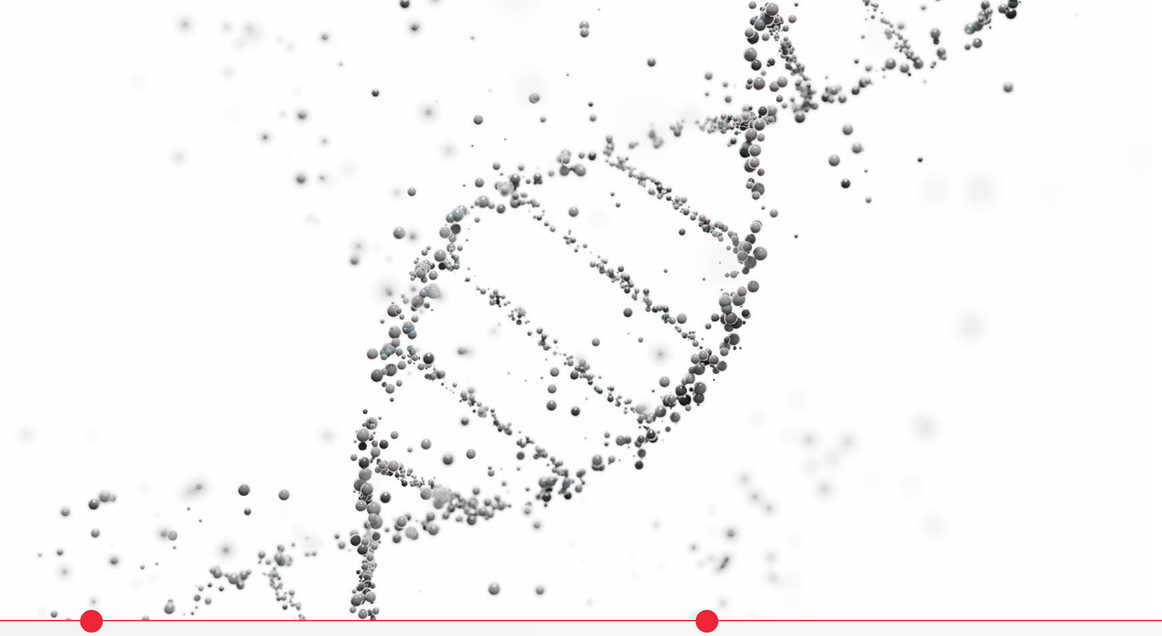
Automated response capabilities for common risk scenarios, enabling swift mitigation without constant manual intervention.

Contextual security awareness integrated directly into workflows, providing guidance at the moment of risk without disrupting productivity.

Reduced security analyst burden through intelligent automation, allowing your team to focus on strategic initiatives rather than routine alerts.

Days 61-90: Optimisation & Resilience

The final phase focuses on refining processes, measuring effectiveness, and building sustainable resilience.



Analyse Protection Effectiveness

Measure changes in human risk metrics since implementation, identifying areas of improvement and persistent challenges. This analysis should evaluate both technical efficacy and employee behavioural changes, providing insight into overall programme effectiveness.

Optimise Security Workflows

Adjust protection mechanisms based on operational impact and risk reduction. This continuous refinement ensures that security measures remain appropriate to actual threats without creating unnecessary friction for users.

Enhance Integration Across Systems

Strengthen connections between security components, ensuring that intelligence flows seamlessly between email protection, collaboration security, and insider risk detection. This integration enables comprehensive visibility and coordinated response across the entire human risk landscape.

Establish Continuous Improvement Framework

Implement a structured approach to ongoing programme evolution, incorporating feedback from security teams, business units, and employees. This framework should adapt to emerging threats and changing business requirements whilst maintaining core security principles.

TIMELINE

Outcomes by Day 90

By the 90-day mark, you'll have refined your approach and established the metrics to demonstrate real security improvements. This optimisation phase delivers four tangible outcomes:

Quantifiable human risk reduction with metrics that demonstrate the effectiveness of your security initiatives.

Optimised security workflows that provide protection whilst minimising disruption to business operations.

Comprehensive security integration across all systems, creating a unified view of your organisation's security posture.

Continuous improvement framework that ensures your programme evolves alongside emerging threats and changing business requirements.

BEYOND TECHNOLOGY

The Human-Centric Approach

Effective human risk management extends beyond technological implementation. It requires understanding behavioural patterns, recognising organisational context, and creating conditions where secure actions become intuitive rather than burdensome.

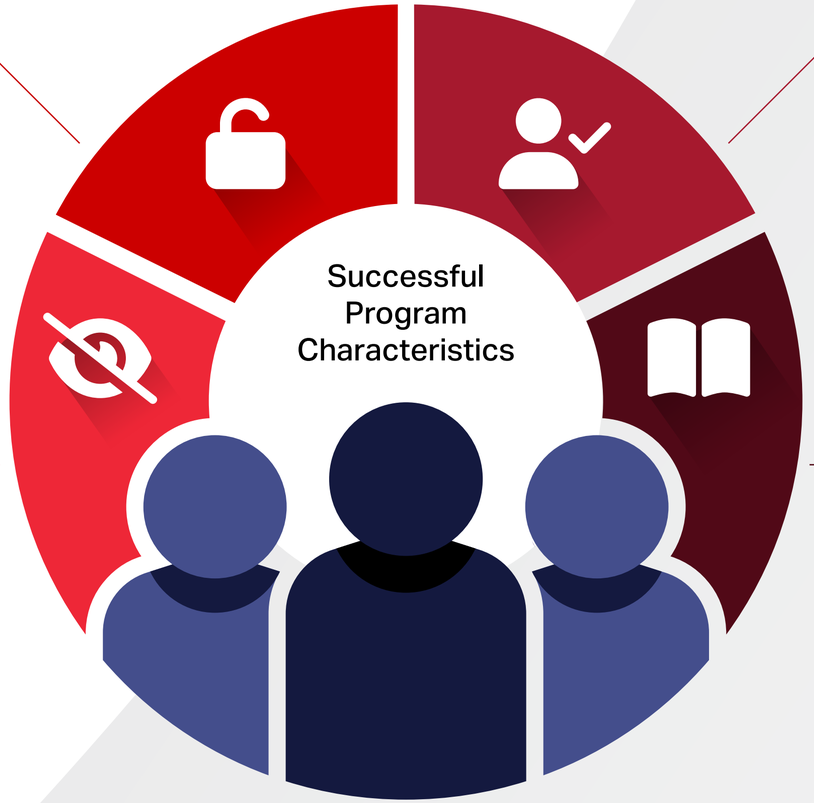
The most successful programmes share several characteristics:

Protection Without Restriction

They implement meaningful safeguards that stop actual threats whilst enabling legitimate business activity. Security becomes a business enabler rather than a limitation, supporting productivity instead of impeding it.

Visibility Without Invasion

They provide comprehensive insight into risk patterns without excessive monitoring or privacy concerns. Employees understand that security measures exist to protect both corporate assets and their own professional reputations.



Accountability Without Blame

They create cultures where security responsibility is shared across the organisation. When incidents occur, the focus remains on improvement rather than punishment, encouraging transparency and cooperation.

Education Without Overload

They deliver relevant security guidance at the moment it matters most. Rather than overwhelming employees with comprehensive training sessions, they provide targeted information when specific risks emerge.

CDW & MIMECAST

A Smarter Approach to Human Risk Management

Security isn't just about having the right technology—it's about making it work for your organisation. That's where CDW and Mimecast come together to provide a seamless, practical approach to tackling insider risk.

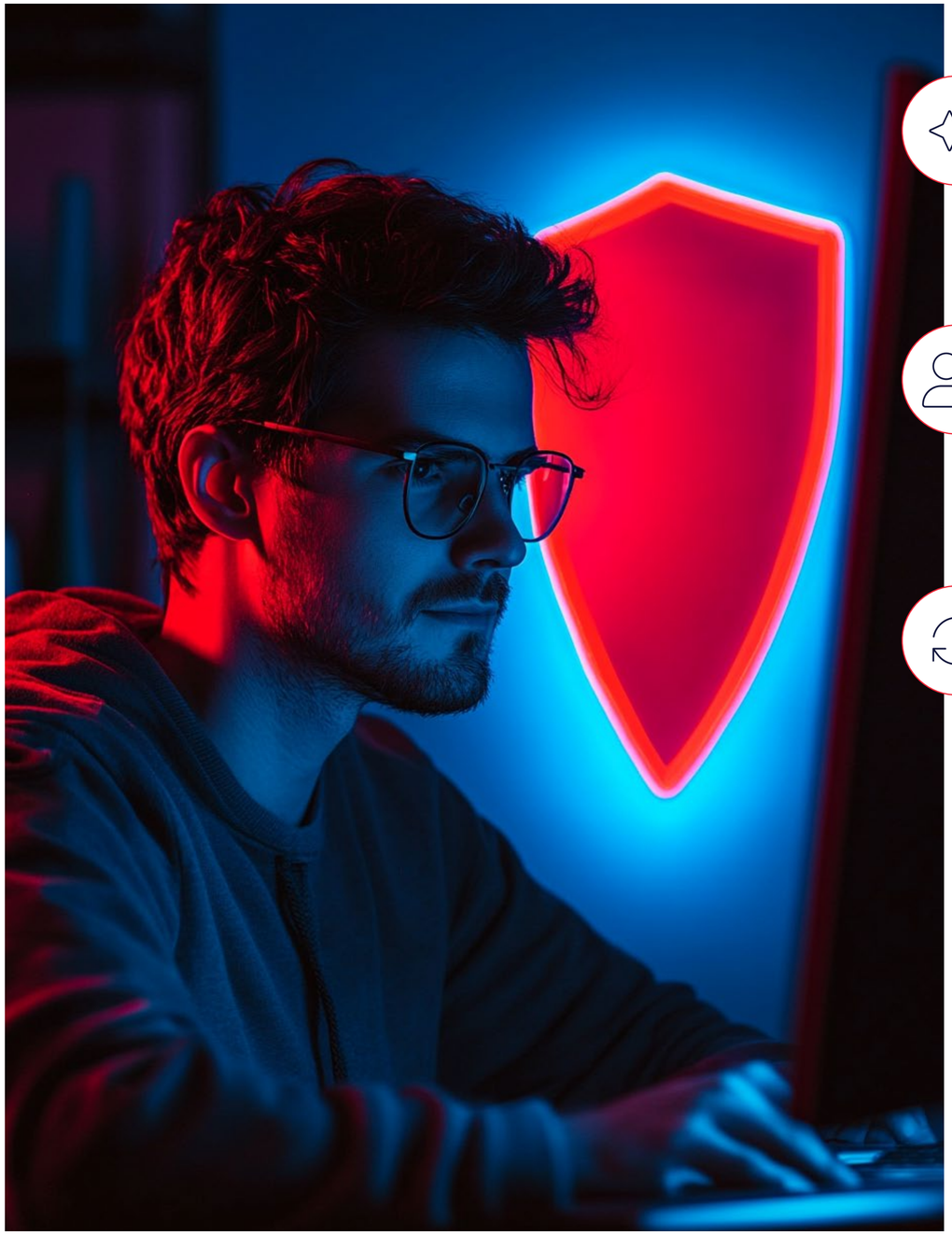
CDW brings deep expertise in security implementation, integration, and strategy, ensuring solutions are tailored to your business without unnecessary complexity.

Mimecast delivers advanced security technology that underpins this approach—providing the intelligence and automation needed to secure email, collaboration, and insider risk.

Together, CDW and Mimecast make security intuitive, effective, and easy to manage.

A Practical, People-First Approach

Traditional security methods can create roadblocks, making it harder for employees to do their jobs. Our approach is different:



Seamless Implementation

CDW ensures that Mimecast's security solutions integrate smoothly with your existing infrastructure, reducing operational disruption.

Security That Works for People

Instead of restrictive policies, we provide real-time guidance that helps employees make secure decisions without frustration.

Ongoing Protection & Support

CDW's security specialists harness Mimecast's AI technology, which analyses 7 billion daily signals to stop threats before they reach users. This protection covers all collaboration channels—email, file sharing, messaging, and cloud storage—ensuring your teams are protected, and staying ahead of evolving threats.

Security shouldn't slow you down—it should empower your business. With CDW and Mimecast, you get a proactive, tailored approach that transforms insider risk into resilience.

CONCLUSION

Security as an Enabler

Security should never feel like an obstacle. The most effective cybersecurity programmes make protection effortless, integrating security into daily workflows so it feels natural.

By following this 90-day roadmap, organisations can move beyond reactive security measures and build a culture of resilience—where employees are an active part of the defence strategy rather than a risk factor.

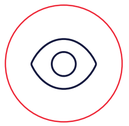
The result? Stronger security, improved productivity, and a business that's ready for whatever comes next. When security becomes second nature, employees become your strongest defence, not your biggest vulnerability.

TAKE ACTION

Secure Your Business with a Tailored 90-Day Plan

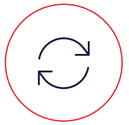
Every organisation faces unique security challenges based on its structure, industry, and risk profile. CDW and Mimecast offer customised human risk management strategies that address your specific requirements whilst following proven implementation principles.

Contact us today to develop a tailored 90-day plan that transforms human risk into your strongest security asset. Our joint approach delivers:



A comprehensive risk assessment that identifies your most pressing vulnerabilities

A customised implementation strategy based on your specific business requirements



Ongoing optimisation to ensure continuous improvement and maximum ROI

By partnering with CDW and Mimecast, you gain more than technology, you gain strategic advisors dedicated to making security work for your business rather than against it. Our team will guide you through each phase of implementation, ensuring maximum value and minimal disruption as you transform your approach to human risk.

Let us focus on the constantly evolving security landscape, so you can focus on your business.

Contact us