mimecast

Ransomware: Defending against costly collaboration attacks

WHITEPAPER

To understand and block ransomware, security leaders must shift their focus to human risk, adopting an actionable framework for understanding, mitigating, and recovering from ransomware.

Introduction

Just 8% of employees are responsible for 80% of ransomware incidents.

Human risk has surpassed technology gaps as the biggest cybersecurity challenge for organizations around the globe, as demonstrated in *Mimecast's State of Human Risk 2025*[1] *report*. Based on interviews with 1,100 IT security and IT decision makers, despite having spent billions to strengthen technology stacks, breaches continue unabated, mostly due to human risk. In fact, insider threats, credential misuse, and human missteps now account for most security incidents.

The key takeaway? Humans remain the weakest link in cybersecurity, with 60% of breaches involving human risk. **Of these breaches, just 8% of employees are responsible for 80% of incidents**[2]**.**

CISOs, CIOs, and other security leaders must be equipped with the tools needed to counter ransomware attacks. This white paper examines how human risk, coupled with evolving attack methodologies, amplifies vulnerability. Learn how to apply adaptive, multi-layered defense strategies and effective human risk management (HRM) to mitigate cyber risks, minimize organizational impact, and ensure business continuity.

[1] State of Human Risk 2025 Report, 2025
[2] Exposing Human Risk, ebook, 2024

Ransomware remains a top cyber risk

44%

breaches involve ransomware

Ransomware has solidified its position as a top cyber risk. According to the 2025 Verizon Data Breach Investigations Report[3] (DBIR), ransomware was involved in 44% of breaches. Ransomware does not just lock systems; it disrupts operational continuity, impacts revenue, and erodes trust.

Ransomware does not just target systems; it attacks people when those systems are compromised. In healthcare, for example, ransomware targets people who rely on systems to survive.

A ransomware attack could delay vital surgeries, putting lives at unnecessary risk. Emergency rooms can potentially halt when healthcare systems are paralyzed by ransomware. For patients awaiting urgent care, every second lost to a ransomware attack could mean the difference between life and death. When hackers encrypt health records, the most vulnerable patients suffer the most. The human cost of a ransomware attack in healthcare extends beyond numbers; it is about lives being disrupted and at risk due to delayed care.

[3] 2025 Verizon Data Breach Investigations Report (DBIR), 2025

Protecting people requires more than training

Protecting people requires more than training. It demands visibility into behavior and intent. The DBIR delivers a clear warning: 60% of breaches[4] involve human risk, whether through error, manipulation, or malicious misuse. Protecting people requires comprehensive strategies, moving beyond basic tools to focus on behavioral insights, custom training, and adaptive actions that address risky user behavior.

By integrating individuals, technology, and workflows, organizations can build strong cyber resilience and safeguard themselves from the constantly changing threat environment. When it comes to ransomware, risky behaviors such as not patching a machine or having bad click hygiene can enable a ransomware attack.

Employees often delay or ignore software updates, leaving systems vulnerable to known vulnerabilities. Cybercriminals use these security weaknesses as entry points for ransomware attacks.
For instance, an unpatched web browser on an employee's device is exploited through a vulnerability that allows ransomware to bypass security protocols.

Phishing is one of the most common ways ransomware infiltrates systems. Cybercriminals deceive employees into clicking malicious links or attachments, exposing the organization's network to ransomware.
For instance, if an employee receives an email disguised as a message from the IT department asking to verify login credentials, clicking the link, and submitting details can enable attackers to deploy ransomware on the network.

60%

breaches involve human risk

Prevention tip

Automate software updates across all devices and emphasize the importance of staying up to date.

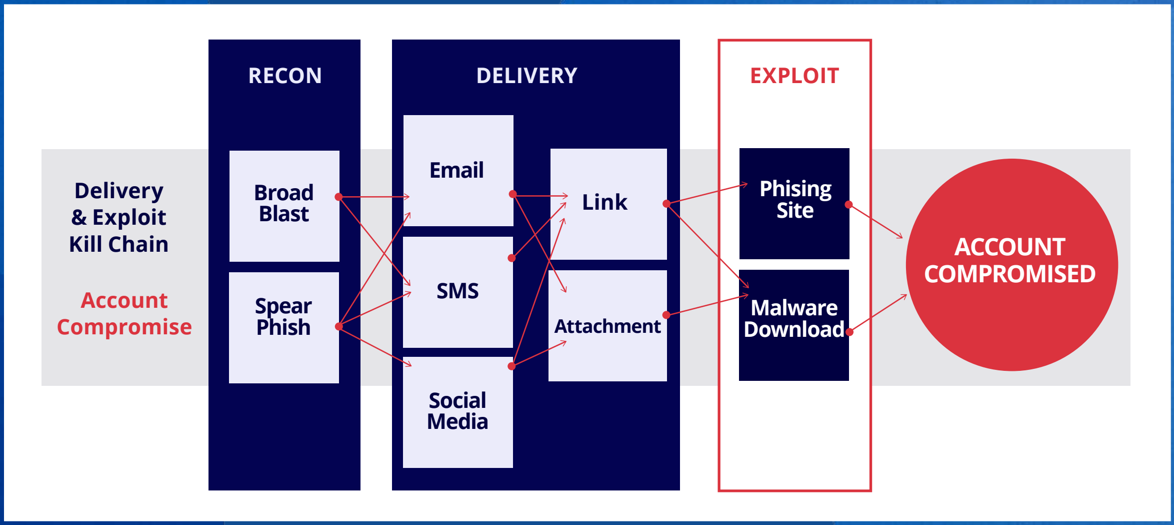
Prevention tip

Train employees to recognize phishing attempts and encourage them to verify suspicious emails or messages with IT directly.

[4] Verizon: 60% of breaches involve human error, blog, 2025

Measuring behaviors that enable kill chains

Account takeover



Ransomware

Human factors in successful ransomware kill chain

- **Phishing click or browsing to bad site**
- **Download and execute file**
- **Unpatched machine**
- **Back-up not enabled**

Collaboration-based cyberattacks, specifically ransomware attacks, have become one of the most significant threats organizations face. These sophisticated attacks, which infiltrate email, chat, and file-sharing systems, originate and thrive on human risk. And by leveraging advanced techniques like generative AI and obfuscation, ransomware campaigns evolve at lightning speed.

By aligning people, technology, and processes, organizations can achieve effective cyber resilience and protect themselves against evolving threat landscapes.

The expanding threat of ransomware

Ransomware has rapidly evolved, diversifying its entry points and broadening its reach. Collaboration applications like email, chat platforms, and document-sharing tools have become gateways for devastating attacks, especially with increasing remote and hybrid work models. Cybercriminals exploit human risk, leveraging collaboration tools like Slack or Microsoft Teams to infiltrate organizations and create havoc.

The increase in ransomware prevalence is impossible to ignore.

Ransomware was involved in **44%** of breaches in 2025 (Verizon DBIR)

SMBs face a disproportionate burden, with **88%** of ransomware breaches affecting them, compared to just **39%** for larger organizations

5. 2025 Verizon Data Breach Investigations Report (DBIR), 2025

High-profile ransomware attacks

High-profile attacks on organizations such as Marks & Spencer, Co-op[6] and others further underscore the financial and reputational costs of ransomware. These targets are often crippled, with operational infrastructures and customer relationships left in shambles.

The modern threat landscape and rising ransomware trends.

The threat landscape has evolved dramatically in recent years, with ransomware emerging as one of the most pervasive and damaging cyber threats. Attackers are no longer just opportunistic actors; they are well-funded, organized, and strategically targeting sectors such as retail, healthcare, education, and critical infrastructure. The rise of Ransomware-as-a-Service (RaaS[7]) has democratized cybercrime, enabling even less technically sophisticated actors to launch devastating attacks. Combined with evolving encryption techniques, data exfiltration, and double extortion tactics, these trends show no signs of slowing down.

How human and systemic vulnerabilities elevate risks.

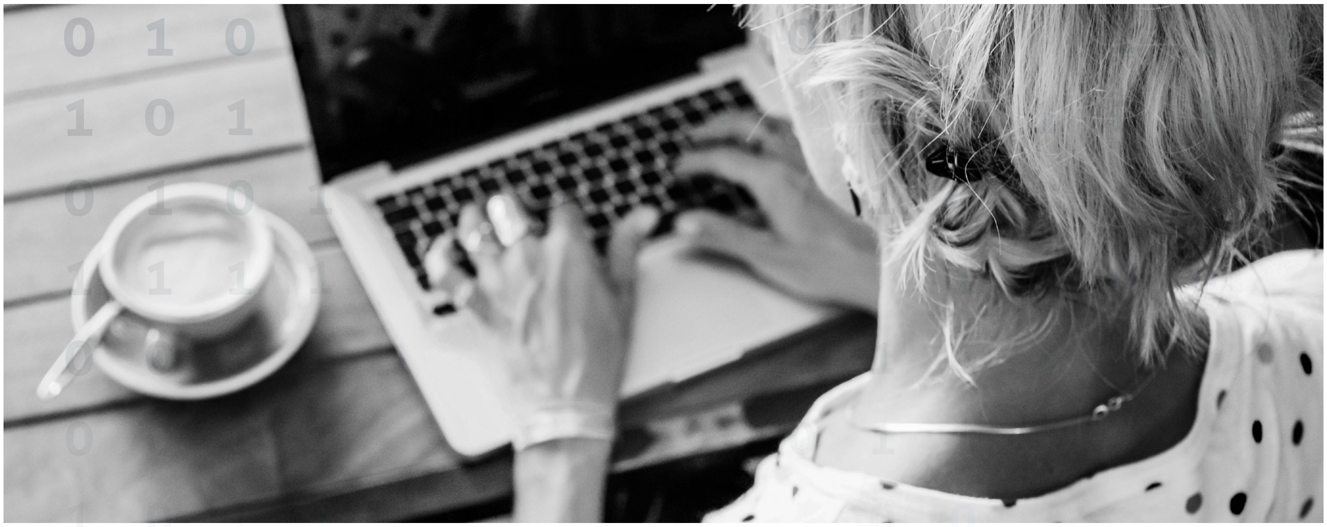
Despite increasing investments in cybersecurity, organizations remain vulnerable due to a combination of human error and systemic weaknesses. Systemic issues, such as overly complex IT environments, outdated legacy systems, and insufficient incident response planning, create blind spots that attackers can easily exploit[8]. Cybersecurity is not just a technical problem; it is an organizational challenge that spans people, processes, and technology.

A resilient framework for mitigation, prevention, and recovery, combining advanced threat prevention with a focus on mitigating human risk.

To effectively combat ransomware, organizations must adopt a holistic, resilient cybersecurity framework. Data loss prevention (DLP) policies[9] are safeguards that organizations establish to protect sensitive data from unauthorized access or data leaks. This includes deploying next-generation firewalls, endpoint detection and response (EDR), network segmentation, and real-time threat intelligence to proactively block attacks. It also includes prioritizing cybersecurity awareness training, phishing simulations, and a strong security culture to reduce the likelihood of human error.

[6] Human Error at the Heart of Recent Ransomware Attacks on UK Retail Giants, blog, 2025
[7] Ransomware Attacks, Mimecast.com, 2025
[8] Human Risk Management: Why it's Time to Re-Envision Awareness Training, blog, 2024
[9] Why Your Business Needs a Data Loss Prevention Security Policy, blog, 2025

Escalating ransomware prevalence



88%

data breaches were SMBs

Ransomware's share of data breaches rose from 32% in 2024 to 44% in 2025[10], reflecting both the sophistication and operational focus of attackers. SMBs remain disproportionately targeted, comprising 88% of these breaches due to their typically weaker security postures. Retail giants in the UK, including Marks & Spencer and Harrods[11], served as recent cautionary tales following operational shutdowns caused by collaboration-based attacks.

[10] 2025 Verizon Data Breach Investigations Report (DBIR), 2025

[11] Human Error at the Heart of Recent Ransomware Attacks on UK Retail Giants, blog, 2025

Modern attack techniques

Ransomware attacks increasingly leverage sophisticated techniques designed to exploit human risk and avoid detection:

Phishing and obfuscation

Over 3.4 billion phishing emails are sent daily, with a sevenfold increase in QR code-based phishing („quishing“) compared to last year[12]. These attacks bypass traditional email filters and exploit mobile user behavior, making them harder to detect and easier to scale.

Ambient ransomware

These attacks seamlessly blend into workflows, penetrating through messaging systems and integrations. Collaboration platforms like Slack, Zoom, and Microsoft Teams, along with email tools, have become engrained in how employees interact daily and a vital part of how they collaborate to complete their tasks. Unfortunately, however, cybercriminals know how much these collaboration tools are being used and target these everyday interactions between employees to compromise organizations.[13]

Shift in objectives

Modern attacks increasingly aim for data extortion and business disruption[14] rather than encryption alone. Threat actors now often exfiltrate sensitive data and threaten to leak or sell it, amplifying pressure on victims and increasing their willingness to pay.

Generative AI (GenAI)

Cybercriminals now use AI[15] to craft highly tailored phishing emails and evasive ransomware payloads, as well as to weaponize stolen data. Cybercriminals are leveraging GenAI to automate and personalize attack content at unprecedented levels. AI tools are used to craft convincing spear-phishing emails, generate polymorphic malware, and even analyze and weaponize stolen datasets. This dramatically reduces the time and skill needed to launch a successful campaign, while increasing its effectiveness.

Ransomware-as-a-Service (RaaS)[16]

RaaS enables even non-technical affiliates to deploy sophisticated attacks at scale, accelerating the threat landscape. The commoditization of ransomware through RaaS platforms has lowered the barrier to entry for cybercrime. Even individuals with minimal technical skills can now launch sophisticated ransomware attacks by purchasing or subscribing to pre-packaged malware kits. These services often include customer support, dashboards, and payment handling, accelerating the spread and volume of attacks globally.

[12] Quishing Takes Advantage of Popular Marketing Tool, blog, 2024
[13] The State of Human Risk: Email and Collaboration Threat Protection, blog, 2025
[14] Data Exfiltration: What It Is and How to Prevent It, blog, 2024
[15] Mimecast Threat Intelligence: How ChatGPT Upended Email , blog, 2025
[16] Ransomware Attacks, Mimecast.com, 2025

Key challenges facing security teams

Email and collaboration tools including Slack, Microsoft Teams and Zoom serve as the point of entry for the majority of cyberattacks.[17] As BEC, phishing and brand impersonation become more advanced, technology must evolve to address these threats and the human risk that opens the door to them. Specific challenges include:

Detection and response limitations

Attackers continually evolve delivery mechanisms, rendering traditional detection tools less effective. Obfuscated malicious links are now more common than attachments, increasing the need for sophisticated detection at the click-point. (Global Threat Intelligence Report H2 2024[18]).

Maintaining operations amid attacks

Ransomware-induced downtime in collaboration systems can lead to immediate revenue loss, exemplified by Marks & Spencer's operational disruptions.[19] Security teams often struggle to balance business continuity with aggressive mitigation efforts.

Data recovery and business resilience

The speed of recovery is critical to mitigating financial and reputational damage. Swift restoration of emails and business-critical files determines the level of operational impact post-incident.

[17] Email & Collaboration Threat Protection, Mimecast.com, 2025
[18] Global Threat Intelligence Report H2 2024
[19] Human Error at the Heart of Recent Ransomware Attacks on UK Retail Giants, blog, 2025

Critical components of defense

By merging people, technology, and processes, businesses can build robust cyber resilience and safeguard against the constantly changing threat landscape. While advancements in technology have fortified defense strategies, the human factor remains a critical component that cannot be overlooked.

Key human risk elements and how organizations can mitigate these risks to enhance overall security and operational efficiency include:

- **Threat intelligence integration across tools like SIEM and XDR[20]**
- **User risk profiles identifying high-risk individuals and roles**
- **At-time-of-click threat analysis to block obfuscated threats**
- **Adaptive, granular controls tailored to specific users or departments**

[20] SIEM vs. SOAR vs. XDR vs. UEBA: How Are They Different?, blog, 2024

Foundations of a strong collaborative defense against cyber threats

Collaboration tools like email, messaging platforms, and shared workspaces are vital to productivity. They also present attractive targets for cyber attackers. Organizations must go beyond traditional security measures to create a layered, strategic defense specifically designed for collaborative environments. A modern defense strategy integrates proactive threat detection, user awareness, business continuity planning, and swift incident response to counter increasingly sophisticated attacks. Essential components for building a resilient, adaptive collaboration security framework that protects both infrastructure and end users include:

Advanced Threat Prevention[21]

Advanced Threat Protection is a comprehensive, cloud-based enterprise-grade protection solution to guard email systems from a range of cyberattacks such as spam, viruses, and malware. As cyber threats constantly evolve it is crucial for organizations of all sizes to implement and layer on advanced threat protection solutions such as:

- Real-time filtering of phishing and brand impersonation, or account compromise, threats
- Protection against both links and attachments
- Sandbox analysis to detect encrypted and polymorphic threats
- Behavioral analytics to identify anomalies pre- and post-delivery

Security Awareness and Training[22]

Mitigate real risk and revolutionize security awareness with a human-centric approach in the following ways:

- Implement customized training for high-risk users
- Conduct simulated phishing and social engineering exercises
- Track and analyze "near miss" incidents reported by users

[21] Advanced Threat Protection, Mimecast.com, 2025

[22] Security & Awareness Training, Mimecast.com 2025

Operational Continuity and Data Resilience [23]

A cyber incident can disrupt an organization's operations, leading to downtime, financial losses, reputational damage, and potential legal and regulatory consequences. Cyber resilience plays a vital role in this context and ensures that an organization can continue its critical functions even during or after an incident, reducing disruption to business operations.

- Ensure continued access to email and collaboration tools, even during attacks
- Automate frequent backups and validate data integrity
- Develop rapid failover processes for seamless incident recovery

Incident Response, Remediation, and Recovery [24]

- Automate workflows to streamline investigations for faster response rates
- Ensure effective internal communication during an attack
- Restore critical systems with minimal downtime to mitigate economic loss

[23] Definition of cyber resilience, Mimecast.com, 2025

[24] What is threat detection and response? Mimecast.com 2025

Measuring success and ROI

Security efforts can be quantified through several metrics[25], including:

- Reduction in financial damage from breaches
- Faster recovery times and reduced downtime post-attack
- Metrics for user risk scores, breach impact reduction, and compliance KPIs

Identifying human risk and establishing more resilient defenses have become essential in any organization's daily operations. Yet, the path to protection may not be linear. While there is no universal consensus on which techniques an enterprise should use to track progress, organizations that identify their risk tolerance and then assign KPIs are far more likely to build a better HRM program than those that do not.

Improving Human Risk Management and cybersecurity operations requires focus, vigilance, the right technology, and proven training methods. Identifying useful metrics and achieving adequate visibility to apply them across all an organization's IT and security assets, as well as across all users, can be challenging. But organizations that understand which metrics really matter for specific groups, as well as the KPIs that drive performance overall, are equipped to reduce risk and avoid potentially crippling attacks.

[25] Top 10 Cybersecurity Metrics and KPIs, blog, 2024

Why ransomware's growth in the digital realm is unchecked

Ransomware has become one of the most popular forms of cybercrime in the last decade. Its growth in the digital realm is unchecked and developing technologies only make it easier for cybercriminals to disappear without a trace.

Such technologies include:

AI and machine learning

AI-powered malware can adapt its behavior dynamically, evade detection by traditional security software, and optimize the timing and targets of attacks.

Cloud and remote access exploitation

Increased reliance on cloud services and remote work environments offers new attack surfaces for ransomware to exploit vulnerabilities remotely and spread faster.

Stealth techniques (fileless malware, living-off-the-land binaries)

Malware that resides in memory or uses legitimate system tools helps attackers avoid detection by antivirus and endpoint security solutions.

Advanced encryption techniques

New and stronger encryption algorithms allow ransomware to lock files more securely.

Anonymous payment methods (cryptocurrency).

Cryptocurrencies like Bitcoin and Monero enable cybercriminals to receive ransom payments anonymously, making it difficult for authorities to trace the money.

Dark web marketplaces and tools

The rise of sophisticated darknet marketplaces provides easy access to ransomware-as-a-service (RaaS), letting less technical criminals launch attacks by renting ransomware tools.

Future threats and strategic foresight

Ransomware is a persistent threat, and recent attacks highlight how human risk often serves as a key vulnerability. Strengthening defenses requires a focus on preventative measures, equipping employees with the knowledge and tools to reduce errors and closely monitor unusual activity.[26]

Organizations must prepare for the inevitable evolution of ransomware attacks, including:

- AI-driven collaboration attacks such as synthetic collaborators infiltrating Slack or Teams
- Evasive delivery methods like prompt injections
- Legacy credential exploitation, potentially through forgotten integrations

[26] Getting started: How to protect against ransomware, Mimecast.com, 2025

Mitigating human risk in defense systems requires a comprehensive approach that extends beyond individual training into organizational structure, technology integration, and cultural alignment. While technological advancements continue to revolutionize defense capabilities, human elements like creativity, critical thinking, and adaptability remain irreplaceable assets. Addressing human risk effectively will ensure that defense strategies are not just resilient but also agile in adapting to the rapidly evolving global threat landscape.

To secure business continuity and operational success in the future, addressing ransomware requires an adaptive strategy that fuses proactive prevention with rapid recovery. The most pressing need? Human Risk Management. By educating employees, securing collaboration points, and embedding proactive cyber resilience, organizations can rise to meet this growing threat landscape head-on.

Mimecast offers a multi-layered approach to detect ransomware and prevent it from blocking access to email or data[27]. This includes automatically detecting and isolating potential threats, such as suspicious links or email attachments. This also includes empowering employees in your organization to recognize potential threats themselves and comply with basic cybersecurity protocols like setting strong passwords.

By educating employees, securing collaboration points, and embedding proactive cyber resilience, organizations can rise to meet this growing threat landscape head-on.

[27] How human risk leads to ransomware attacks, blog 2025

mimecast®

HUMAN RISK, SECURED.

About Mimecast
Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more.
More visibility. More insight. More agility. More security.