SECURITY WHITEPAPER 2025

Simple Actions for Complex Problems

2025 Security Breaches, Patterns,
Root Causes & Recommendations

$4.44M	60%	44%	30%
Avg Breach Cost	Human Element	Ransomware	Third-Party

Careful Security | Cybersecurity with a Soul

December 2025

Executive Summary

The 2025 threat landscape reveals a striking pattern: despite increasingly sophisticated attack techniques, most breaches still succeed through fundamental security gaps.

This whitepaper distills findings from the Verizon 2025 DBIR (22,000+ incidents), IBM X-Force Threat Intelligence Index, and major breach analyses to identify the simple, actionable measures that would have prevented the majority of 2025's most damaging security incidents.

KEY FINDING

60% of breaches involved human actions that simple controls could have stopped.

The Three Pillars of 2025 Breaches

22%
Credentials
Stolen or weak

20%
Vulnerabilities
Unpatched systems

30%
Third Parties
Supply chain risk

The Simple Actions That Matter

- Enable MFA everywhere
- Patch within 32 days
- Audit third-party access
- Train on phishing recognition

2025 Breach Landscape

The Year in Numbers

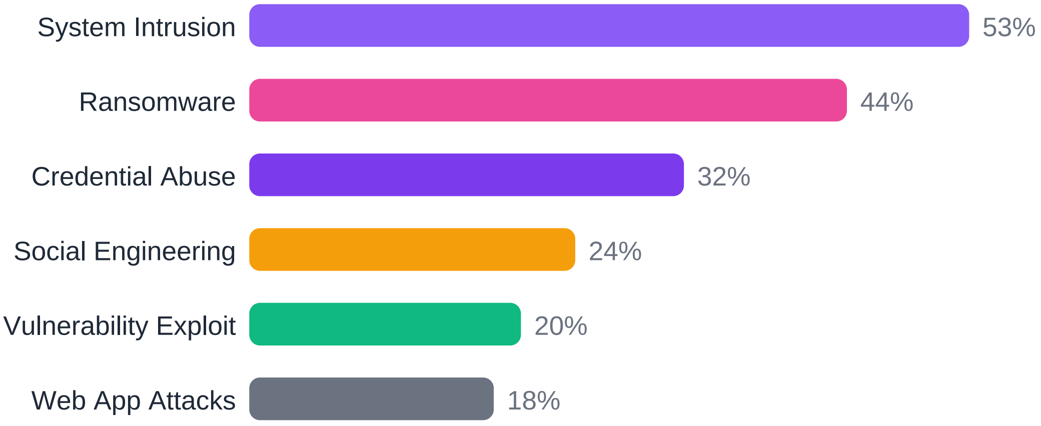
12,195
Confirmed Breaches

$4.44M
Avg Cost per Breach

258
Days to Detect

34%
Vuln Exploitation Up

Top Attack Patterns (% of Breaches)



Most Targeted Industries

26%	**Manufacturing**	4th consecutive year
15%	**Financial**	Highest breach cost
12%	**Healthcare**	$9.77M avg cost

INSIGHT

Third-party breaches doubled YoY to 30% — your vendors' security is your security.

Major 2025 Breaches

A timeline of significant breaches and the simple actions that could have prevented them

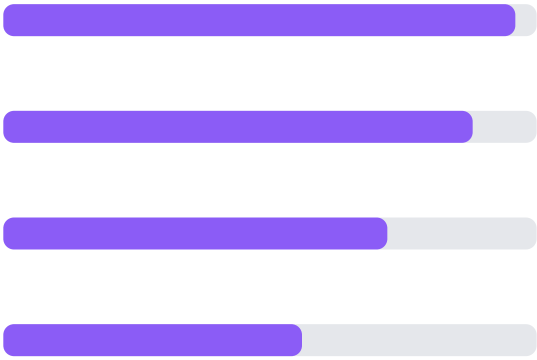
JAN	**PowerSchool**	Impact: 62M student records	Cause: Stolen contractor credentials Fix: MFA + credential rotation
APR	**M&S Retail**	Impact: £300M business impact	Cause: Social engineering Fix: Phishing training + verification
APR	**Blue Shield CA**	Impact: 4.7M customer records	Cause: Google Analytics misconfiguration Fix: Config audits + data classification
APR	**SK Telecom**	Impact: 27M customer SIMs	Cause: Undetected malware (years) Fix: Continuous monitoring + threat hunting
MAY	**Coinbase**	Impact: 69K customer records	Cause: Insider threat via contractor Fix: Least privilege + behavior analytics
JUL	**TransUnion**	Impact: 4.4M individuals	Cause: Third-party Salesforce exploit Fix: Vendor security assessment
JUL	**Allianz Life**	Impact: 1.4M customers	Cause: Third-party CRM attack Fix: Supply chain monitoring
AUG	**Salesloft/Drift**	Impact: 700+ organizations	Cause: Supply chain attack Fix: OAuth token management
SEP	**Jaguar Land Rover**	Impact: Production shutdown	Cause: Ransomware Fix: Network segmentation + backups

Root Cause Analysis

The Human Element: Still the Weakest Link

60% of breaches involved human actions

Source: Verizon 2025 DBIR



Phishing Clicks (24%)
Email links remain the #1 entry point

Credential Misuse (22%)
Weak, reused, or stolen passwords

Misconfigurations (18%)
Cloud and system setup errors

Social Engineering (14%)
Phone/pretexting attacks rising

Technical Failures: The Fixable Problems

- ● **Unpatched Vulnerabilities**
  Median 32 days to patch, but only 54% patched
- ● **Weak/No MFA**
  88% of web app attacks used stolen credentials
- ● **Third-Party Access**
  30% of breaches involved external partners

THE PATTERN

Complex attacks succeed through simple failures. Most 2025 breaches exploited gaps that basic security hygiene would have closed.

2025 Attack Patterns

Ransomware Evolution

44% of breaches

- Double extortion now standard
- Median ransom: $115K
- 64% of victims refused to pay

Supply Chain Attacks

2x YoY increase

- 30% of breaches via third parties
- Salesforce integrations targeted
- SaaS OAuth tokens exploited

Credential-Based Attacks

88% of web app attacks

- Infostealer malware surging
- MFA bypass techniques mature
- Brute force attempts tripled

AI-Enhanced Threats

85% cite AI in attacks

- GenAI phishing campaigns
- Deepfake vishing emerging
- 21% unprepared for deepfakes

Emerging 2025 Threat Vectors

→ **Edge Device Exploitation:** VPN & gateway flaws increased 8x

→ **Infostealer Malware:** 30% of compromised systems had enterprise AV

→ **GenAI Data Leakage:** 15% of employees using AI tools with personal accounts

The 10 Simple Actions

Evidence-based security measures that would have prevented most 2025 breaches

1 **Phishing-Resistant MFA**

Deploy FIDO2/WebAuthn across all systems. SMS OTPs are no longer sufficient.

Blocks 99% of credential attacks

2 **32-Day Patch Cycle**

Establish maximum 32-day remediation window for critical CVEs.

Closes 54% more vuln gaps

3 **Third-Party Access Audit**

Quarterly review of vendor permissions and OAuth integrations.

Reduces 30% breach vector

4 **Zero Trust Architecture**

Verify every access request regardless of source. Trust nothing.

Saves $1.76M per breach avg

5 **Security Awareness Training**

Monthly phishing simulations with real-time feedback.

4x increase in threat reporting

6 **Credential Monitoring**

Subscribe to breach notification services for your domains.

94 days avg secret exposure

7 **Immutable Backups**

Air-gapped, tested backups with 4-hour recovery SLA.

Eliminates ransom leverage

8 **Cloud Config Audits**

Weekly automated scans for misconfigurations.

Prevents 23% of cloud incidents

9 **Incident Response Plan**

Documented, tested IR playbook with clear ownership.

Reduces breach cost $1.49M

10 **Executive Cyber Training**

Board-level understanding of risk and investment needs.

63% cite lack of exec support

90-Day Implementation Roadmap

PHASE 1
Weeks 1-4

Foundation

- Deploy MFA across all critical systems
- Inventory all third-party integrations
- Establish vulnerability scanning ca
- Document incident response contacts

PHASE 2
Weeks 5-8

Hardening

- Implement Zero Trust network segmentation
- Configure immutable backup solution
- Launch security awareness program
- Audit cloud configurations

PHASE 3
Weeks 9-12

Optimization

- Establish vendor security requirements
- Deploy credential monitoring
- Conduct tabletop IR exercise
- Present security metrics to leadership

Week 1 Quick Wins

✓ Enable MFA on all admin accounts today

✓ Review and revoke unused OAuth tokens

✓ Verify backup restoration process

✓ Update incident response contact list

$1.76M **Average savings per breach with Zero Trust implementation**

Organizations using AI-powered security detect breaches 108 days faster — saving $1.9M avg.

Conclusion

The 2025 breach data tells a consistent story: complex attacks continue to succeed through simple security gaps. While threat actors deploy increasingly sophisticated techniques — from AI-enhanced phishing to supply chain compromise — their success still depends on fundamental failures:

- Credentials that should have been protected by MFA
- Vulnerabilities that should have been patched
- Third-party access that should have been monitored
- Employees who should have recognized the threat

60%	30%	$1.76M	108
of breaches involve human element	involve third-party compromise	saved with Zero Trust	days faster detection with AI security

Ready to Take Action?

Careful Security helps mid-market companies achieve
90-day compliance and continuous security.

Get Your Free Assessment →

icare@carefulsecurity.com | +1-818-533-1402 | carefulsec.com