LogMeIn Resolve | Acronis

The 2025 Cybersecurity Playbook for MSPs and IT Teams

Cybersecurity threats are evolving at an unprecedented pace, and the stakes have never been higher. Based on insights from the latest "Practically Tomorrow" podcast episode featuring cybersecurity evangelist Steve Brining from Acronis, this comprehensive guide breaks down the most pressing cyber threats facing MSPs and IT professionals in 2025—and provides actionable strategies to defend against them.

Steve Brining, Technology and Cybersecurity Evangelist at Acronis, shared critical intelligence from the company's latest cyber threat report insights drawn from over 1 million unique endpoints worldwide. A CISSP-certified expert, Brining also serves as a commanding officer in the Arizona Army National Guard and is a member of the FBI InfraGard. The data he presented reveals alarming trends that every IT professional needs to understand.

The landscape has shifted dramatically. Email-based attacks have surged by nearly 200%, AI-driven threats are becoming mainstream, and no organization—regardless of size—is safe from sophisticated cybercriminals. For MSPs especially, the risk is compounded: compromising a single admin credential can provide attackers access to multiple client environments simultaneously.

Understanding the Current Threat Landscape

Insider Threats and Third-Party Risks

Malicious or negligent insiders pose significant risks, along with compromised third-party contractors. These threats can lead to data leakage, sabotage, and access abuse—often going undetected for months.

AI-Driven Cyber Attacks

Artificial intelligence has lowered the barriers to entry for cybercrime dramatically. Tools like ChatGPT, WormGPT, and FraudGPT enable even low-skilled actors to launch sophisticated attacks, including hyperrealistic phishing campaigns and deepfake social engineering.

Fileless Malware and Advanced Persistent Threats

Unlike traditional ransomware, fileless malware operates in memory without writing malicious files to disk, making detection significantly more challenging.

Why MSPs Are Prime Targets

MSPs represent a particularly attractive target for cybercriminals due to their unique position in the technology ecosystem. A successful breach of an MSP can provide attackers with access to dozens or even hundreds of client environments through a single compromised administrative credential.

Small businesses served by MSPs often lack the sophisticated cybersecurity talent and resources of larger enterprises, making them vulnerable to “spray and pray” attack techniques that cast wide nets hoping to catch unprepared victims.

Email Security: Your First Line of Defense

Email remains the primary attack vector, with phishing and malicious emails serving as the main factors for malware infection according to Acronis' threat report.

Critical Email Red Flags to Train Your Team On

Address and Domain Issues

- Slight misspellings in email addresses (such as "support@paypal.com" using "1" instead of "l")
- Use of free domains instead of legitimate company domains
- Spoofed display names hiding malicious underlying addresses

Content and Attachment Warning Signs

- Fear-based language creating false urgency ("Account will be suspended immediately")
- Unexpected zip files, executables, or password-protected attachments
- Double extensions like "document.pdf.exe"
- Malicious URLs where displayed text differs from the actual destination

The Hover Test

Train employees to hover over sender names and links before clicking. This simple action reveals the actual email address and URL destination, often exposing spoofed communications immediately.

Modern AI Phishing Challenges

AI-generated phishing emails present a paradox: they're sometimes so grammatically perfect and professionally formatted that their perfection becomes suspicious. However, this level of sophistication makes them incredibly convincing to untrained eyes.

Implementing Robust Defense Strategies

For Business Leaders and IT Managers

Technical Controls

- Deploy comprehensive email security solutions with advanced threat detection
- Implement multi-factor authentication (MFA) across all systems and accounts
- Regular security assessments of cloud configurations and access controls
- Monitor for unusual insider activity and third-party access patterns

Human-Centered Security

- Conduct regular phishing simulations to test employee awareness
- Provide ongoing cybersecurity training that evolves with the threat landscape
- Establish clear, simple procedures for reporting suspicious emails
- Create and regularly test incident response plans

The Three-Point Employee Training Framework

Based on Steve Brining's recommendations, focus employee training on these three critical checkpoints:

1. **Attachment Awareness:**
Question every unexpected attachment, especially executable files or compressed archives

2. **URL Verification:**
Always hover over links to verify destinations before clicking

3. **Sender Authentication:**
Check that email addresses match the claimed sender organization

Advanced Threat Considerations

State-Sponsored and Organized Crime

Cybercriminal organizations from China, Russia, Iran, and North Korea are increasingly targeting critical infrastructure including healthcare, energy, transportation, and education sectors. These groups employ sophisticated techniques including:

- Ransomware with double or triple extortion models
- Cloud infrastructure exploitation through misconfigured services
- IoT and operational technology (OT) exploitation with potential physical world impacts
- Distributed denial of service (DDoS) attacks available as hired services

The AI Arms Race

The cybersecurity community is responding to AI-driven threats with AI-powered defenses. The best offense truly is a strong defense, and organizations must leverage artificial intelligence to fight AI-enhanced attacks.

Modern defense strategies include machine learning-based threat detection, behavioral analysis systems, and automated response mechanisms that can identify and neutralize threats faster than human analysts.

Building Cyber Resilience

Beyond Insurance: Taking Responsibility

While cyber insurance provides important financial protection, it has limitations. Organizations cannot rely solely on insurance coverage—they must take proactive responsibility for implementing robust cybersecurity measures.

Quarterly Security Hygiene

Implement a quarterly reminder system to review and update:

- Device firmware and software patches
- Access controls and user permissions
- Backup and recovery procedures
- Security policy compliance across all systems

LogMeIn Resolve | Acronis

Protecting Your Organization with LogMeIn Data Protection Suite

For MSPs and IT teams, keeping client environments secure and operational is non-negotiable. **LogMeIn Data Protection Suite,** powered by Acronis, offers a modern approach to **backup and disaster recovery (BCDR)**—purpose-built for the demands of today's threat landscape.

This all-in-one solution combines **secure cloud and local backup, fast data recovery,** and built-in **anti-ransomware protection**—so you can keep systems running, reduce recovery time, and maintain business continuity, even in the face of outages or attacks.

Whether you're supporting SMBs or enterprise environments, LogMeIn Data Protection Suite helps you deliver reliable, secure, and efficient BCDR—without the headache.

Explore how you can simplify and strengthen your BCDR offering with LogMeIn Data Protection Suite powered by Acronis. Learn more about LogMeIn Data Protection Suite powered by Acronis