MFA Was Never Meant to Be Enough

Why Layered Security Matters More Than Ever

Mike Giovaninni | NetWerks Strategic Services, LLC

The frequently heard cry of "We have MFA" is a growing sign of the times. The question is, what does this really mean?

For a business owner discussing cybersecurity with their IT provider, that is a good answer to an important question. Multi-factor authentication remains one of the most effective controls available for reducing the risk associated with stolen passwords and compromised accounts. CISA continues to recommend that businesses require MFA wherever possible and move toward stronger, phishing-resistant forms of authentication.

The problem begins when "we have MFA" becomes shorthand for "our identities are protected."

They aren't necessarily the same thing.

Cybersecurity controls are layers, not guarantees. MFA was designed to make it harder for someone possessing a username and password to impersonate the legitimate user. It was never intended to protect every part of the identity lifecycle, every device a user works from, every authenticated browser session, or every cloud application the business relies upon.

Attackers understand those limitations and actively pursue the means to exploit what has become a level of complacency that masks the often overlooked danger.

As a result, businesses need to understand these limitations as well.

In This Brief

MFA remains essential for identity management, and yet is still subject to vulnerabilities. Attackers are increasingly targeting what happens before and after authentication.

This brief examines:

- session theft
- browser risk
- identity controls
- layered security
- business risk

The Attack Doesn't Have to Defeat MFA

Traditional phishing was relatively straightforward. An attacker created a convincing email with links that pointed to a well-crafted fake login page, persuaded someone to enter a username and password, and collected the credentials.

While MFA made the authentication process considerably more difficult, it didn't take long for attackers to adapt.

Modern adversary-in-the-middle phishing can insert attacker-controlled infrastructure into the authentication process. The user may enter legitimate credentials and successfully complete MFA, but the attacker covertly captures the authenticated session information created during that process. That filched session information is valid until the session expires, is revoked, or is otherwise invalidated.

Microsoft documented this behavior again in a 2026 phishing campaign that targeted more than 35,000 users across over 13,000 organizations in just three days. The attack ultimately led victims through a legitimate sign-in experience where adversary-in-the-middle techniques allowed attackers to capture authentication tokens that could provide immediate account access.

The important distinction is easy to miss:

> **The attacker did not necessarily break MFA. The attacker stole the result of a successful authentication.**

It would be unreasonable to expect the user to authenticate with MFA each time they opened an email, saved a document, or performed a routine task. In the current environment, once the user has successfully authenticated, the application provides the user with a trusted session.

That session token has value.

If an attacker can steal or hijack it, the application may see what appears to be an already authenticated user. Microsoft identifies malware and adversary-in-the-middle attacks among the methods attackers use to steal tokens and session information.

This is why the cybersecurity conversation must extend beyond passwords and MFA.

MFA Bypass at Scale

500,000+ organizations per month

Microsoft reported that the Tycoon2FA phishing-as-a-service platform enabled tens of millions of phishing messages each month, providing MFA-bypass capabilities to attackers who did not need to develop the technology themselves.

Source: Microsoft Threat Intelligence, 2026

The Browser Has Become Part of the Security Boundary

For many businesses, the browser has quietly become the primary workplace.

Email is there. Documents are there. Accounting systems are there. Customer information is there. Banking, CRM platforms, line-of-business applications and administrative portals may all be accessed through the same browser.

The browser also participates in authenticated sessions, accepts extensions, handles downloads and notifications, and interacts with dozens of cloud services. With many cloud-based applications allowing additional tabs to be opened using the same trusted session, the browser becomes a significant source of risk.

The value of the trusted session token makes it a prime target of cyber criminals.

In our own work supporting small and midsized businesses, we have encountered unexpected browser software and rogue security-notification activity appearing on endpoints where users had little or no recollection of installing or authorizing it.

That does not necessarily mean the browser itself was responsible for an account compromise. It does mean that unexpected changes to the environment can happen without any participation on the part of the user. The potential for "drive-by" alterations to the browser environment deserves attention.

Each component of the authentication process has a role to play: The endpoint provides the platform, the browser provides accessibility to many modern apps, and the identity configuration determines how much the user can access. While the browser's ability to manage trusted session information is, in a word, elegant, and allows for better application functionality, there is a less obvious downside.

From a threat perspective, that trusted session information can become a valuable target, often without giving the user any indication that it has been accessed or compromised.

HP Wolf Security has documented this growing focus on session cookie theft, noting that attackers can use a stolen authentication cookie to take over an active session without first defeating the user's MFA.

Every aspect of the authentication chain matters, including what happens after authentication succeeds. The threat actor no longer needs to have compromised the endpoint. They may be able to establish an authenticated session from another system without repeating the original authentication process.

Protecting only one piece of the authentication chain leaves the others outside the conversation and vulnerable.

AI Hastens the Threat Cycle

Artificial intelligence deserves a place in this discussion, but perhaps not the place the headlines often give it.

AI did not invent phishing, credential theft, social engineering or malicious websites. It can, however, make those activities easier to scale and harder for users to recognize.

Poor grammar and awkward wording were once useful warning signs of a phishing message. Attackers now have inexpensive tools capable of producing polished business correspondence, translating messages, researching

potential victims, and tailoring social-engineering campaigns.

Common AI tools are able to take examples of the writing styles of key individuals within a company from email, social media, and web content and turn them into convincing business email compromises and phishing campaigns.

Despite these advances, the underlying objective has not changed.

The attacker still needs someone or something to grant access that should not have been granted.

AI may make the invitation considerably more convincing. To that point, recent threat research supports that trend, with the 2026 Verizon DBIR reporting a 40% increase in successful mobile social-engineering attacks.

That makes good security awareness more important, but it also demonstrates why employee training cannot carry the entire burden either.

The employee is a vital layer in the equation. Industry studies consistently show that the human element remains involved in a significant percentage of successful cyberattacks. Not from a malicious perspective, but rather the result of a lack of knowledge on how to spot the levels of sophistication that AI has added to the mix.

The "Human Firewall" is an important part of the overall security tapestry being woven. It is far from being the only one.

This Is Why Defense in Depth Exists

The cybersecurity industry talks frequently about "defense in depth," sometimes without adequately explaining what the term actually means.

It does not mean buying every security product available. It does require a well-founded understanding of the nature of the risk present. And that is specific to each organization. While there are always areas of overlap, each business may have very different perspectives on what risk can be tolerated, and which must be mitigated or transferred.

It does mean accepting a simple reality:

> **Every individual security control can fail.**

A firewall is necessary, but a firewall can contain vulnerabilities or be misconfigured.

Remote access may be protected by a VPN, but vulnerabilities in both IPSec and SSL VPN technologies have repeatedly provided attackers with pathways into otherwise protected networks. Joint government guidance has documented cases where exploited VPN vulnerabilities enabled attackers to hijack legitimate sessions and even bypass password and MFA requirements.

Endpoint protection is necessary, but malware can occasionally evade it. In some cases, malware can turn off local endpoint security components while appearing to still be working.

Security awareness training is necessary, but a well-trained employee can still make a mistake.

Security Controls Can Become Attack Surfaces

In Sophos' 2026 ransomware research, **21% of initial compromises occurred through firewalls and 8% through VPNs**.

Source: Sophos State of Ransomware 2026

MFA is necessary, but authenticated sessions can be stolen.

The possibility that each of these controls can fail is precisely why the others exist.

Recent ransomware research illustrates the point. Sophos reported that 79% of the ransomware incidents in its 2026 survey began with an identity-based approach. Among incidents where compromised credentials were identified as the root cause, 97% of affected organizations had MFA deployed in some capacity. The same research found coverage gaps, including VPNs, firewall administration, and legacy applications where MFA was not consistently present.

That does not mean MFA failed 97% of the time.

It means the statement "We have MFA" doesn't tell us enough about the organization's risk or readiness. The question isn't whether MFA works. The question is whether the controls surrounding identity are appropriate to the risks the organization actually faces. This can best be determined by a thorough risk assessment.

MFA Is a Control, Not an Identity Strategy

A more mature identity-security model asks several additional questions.

- What happens when someone successfully authenticates?
- What privileges does that identity possess?
- What device is being used?
- Should that device be trusted?
- Does the location or behavior make sense?
- What cloud applications can the identity reach?
- Would anyone notice if the account suddenly began behaving differently?
- Could the organization quickly revoke its active sessions?

These questions lead naturally to additional layers of protection.

Privileged Access Management can reduce the ability of a compromised everyday account to become a pathway to administrative control.

Conditional Access can evaluate more than whether the user supplied the correct credentials. Identity, device, risk, location and other conditions can influence whether access should be granted or whether additional verification is appropriate.

Cloud and SaaS monitoring can help identify suspicious activity after authentication, when an attacker using legitimate credentials or a stolen session may otherwise resemble an authorized user.

Microsoft 365, Google Workspace, and other cloud platforms also require deliberate security configuration and ongoing hardening. Moving an application or workload into the cloud does not transfer every security responsibility to the cloud provider. In fact, a look at Microsoft's Shared Responsibility Matrix will quickly show that Microsoft is responsible for securing

the underlying cloud service, but many of the controls governing identities, access, data, and tenant configuration remain the customer's responsibility. The tenant account is not set up in a "locked down" state. That is the responsibility of the tenant administrator.

Phishing-resistant MFA can substantially reduce exposure to several of these attack techniques. It does not, however, eliminate the need for the surrounding security layers. CISA specifically recommends prioritizing stronger authentication for privileged users and accounts with broad access to sensitive customer or financial information.

None of these controls replaces MFA.

Each compensates for something MFA was never designed to do by itself.

Start With What Is Actually at Risk

There is an obvious objection to layered cybersecurity:

It costs money.

The reality: Small and midsized businesses do not have unlimited security budgets. Privileged access management, monitoring, endpoint security, risk assessments, hardened cloud environments, employee training and skilled security professionals all carry costs.

While felt more by smaller organizations, regardless of business size, this fact matters. Cybersecurity controls generally appear on the P&L as an expense. Their value becomes easier to understand when weighed against the potential cost of containment, recovery, business interruption, and reputational damage. In that context, the old adage about an ounce of prevention becomes particularly relevant.

Does every business need every layer of cybersecurity? A knee-jerk response of putting every possible control in place is only going to erode cash flow and still leave the business vulnerable. There is no "one-size-fits-all" security model.

Instead, the conversation should begin with risk.

- What information does the business possess? (You can't secure what you don't know about)
- Which systems are essential to continuing operations?
- What regulatory or contractual responsibilities exist?
- What would happen if those systems were unavailable for several days?
- What would unauthorized disclosure of client, patient, employee or financial information mean to the organization?
- What threats are reasonably likely?
- And which controls meaningfully reduce those risks?

A good risk assessment helps leadership answer those questions and identify weaknesses that may otherwise remain invisible.

From there, security spending becomes a business decision rather than a shopping list.

Some risks may justify additional controls immediately. Others may be mitigated over time. In some circumstances, management may consciously decide that the cost of further mitigation exceeds the risk reduction it provides. In other cases, there may be ways to isolate sensitive systems using other mechanisms such as micro-segmenting those assets into an "enclave" environment.

These treatments are legitimate business decisions.

Accepting a risk without knowing it exists is something very different.

The Impact of Culture

No matter how many controls are put in place, their effectiveness is influenced by the culture surrounding them. A security-aware organization helps its people understand how individual decisions can strengthen or undermine the controls designed to protect the business.

Because culture isn't merely employee behavior. Leadership determines whether circumventing a security control is viewed as ingenuity or a problem.

Security Incidents Cost More Than the Cleanup

Cost also needs to be considered from both sides of the equation.

The cost of prevention is visible. It appears in a budget every month. In many cases it increases periodically as control vendors raise their prices.

The cost of a security incident is less predictable and extends well beyond whatever invoice arrives from the incident-response firm.

There may be direct costs associated with forensic investigation, remediation, restoration, legal counsel, replacement systems, regulatory response, insurance deductibles and fraud or extortion.

There are also operational costs.

Employees may be unable to work. Orders may be delayed. Client services may be interrupted. Leadership may spend days or weeks managing the response rather than running the business.

There are human costs. Stress, overtime and burnout do not appear neatly on an incident-response invoice.

Ask Better Questions

"Do we have MFA?" remains a worthwhile question.

It just shouldn't be the last one.

Recovery Has a Price Tag

$1.7 million

Average recovery cost reported by organizations affected by ransomware in Sophos' 2026 survey, excluding ransom payments.

The survey covered organizations with 100 to 5,000 employees, so this should not be interpreted as the expected cost for a small business.

Source: Sophos State of Ransomware 2026

Business leaders should also be asking:

- Where is MFA actually enforced, and does that coverage satisfy our cyber-insurance requirements?
- What type of MFA are we using?
- Are privileged accounts protected differently from everyday user accounts?
- Do everyday users have administrative rights to their desktop or cloud environments?
- Can unknown or unmanaged devices establish trusted sessions?
- What protects the endpoint and browser where authenticated sessions exist?
- How are our Microsoft 365, Google Workspace and other cloud platforms hardened?
- Are we monitoring cloud applications for unusual activity?
- How would we recognize a stolen or abnormal session?
- Can we quickly terminate active sessions following a suspected compromise?
- Does our security awareness program address the attacks employees are encountering today, or are we relying on stagnant training materials?
- When did we last perform a meaningful assessment of our business and cybersecurity risks?

Those questions may expose areas that deserve attention. They may also demonstrate that existing controls are working exactly as intended. Either result is useful.

“Security controls are layers, not guarantees.”

Security controls do not stop evolving once they are installed. Threat actors continually adapt their methods to find ways around those controls. Simply put, cybersecurity maturity is a journey, not a destination. As technology and threats evolve, businesses must adapt with them.

Regularly evaluating the risks they create and the controls used to manage them helps build a security-aware culture. Over time, that awareness becomes the foundation of the organization’s resilience. In today’s threat landscape, that resilience becomes a valuable asset.

In the long run, MFA remains an essential layer of modern cybersecurity. It was simply never meant to carry the entire weight of the security program.

Expecting it to do so may be the greater risk.

Sources & Further Reading

CISA - Require Multifactor Authentication

cisa.gov

Microsoft - Multi-stage AiTM token compromise campaign

microsoft.com

Microsoft - Inside Tycoon2FA

microsoft.com

Sophos - State of Ransomware 2026

sophos.com

Verizon - 2026 Data Breach Investigations Report overview

verizon.com

HP Wolf Security - Attackers Love Cookies: Tracing the Rise of Breaches Involving Session Cookie Theft

hp.com

Microsoft - Shared responsibility in the cloud

microsoft.com

CISA - Enhanced Visibility and Hardening Guidance

cisa.gov

ABOUT THE AUTHOR

Mike Giovaninni, CISSP

Founder, NetWerks Strategic Services, LLC

Mike Giovaninni is the founder of NetWerks Strategic Services and a CISSP with more than three decades of experience in information technology, networking, and cybersecurity. His career has included military communications and network security, defense contracting, and more than 20 years helping small and midsized organizations use technology effectively and securely.

Through NetWerks, Mike works with business leaders to understand technology and cybersecurity in the context of business risk, operations, and organizational resilience. His approach emphasizes practical security, informed decision-making, and solutions appropriate to the risks an organization actually faces.