U.S. Treasury Breach: How to Mitigate Similar Attacks

14 April 2025 - ID G00832990 - 13 min read

By: Peter Firstbrook, Paul Rabinovich

Initiatives:Cyber Risk; Build and Optimize Cybersecurity Programs; Meet Daily Cybersecurity Needs

The U.S. Treasury Department suffered a major breach of sensitive email content due to an administrative account takeover attack. This event is another in a series of high-profile breaches that should motivate every cybersecurity leader to prioritize identity threat detection and response programs.

How can organizations mitigate the risks associated with the recent U.S. Treasury Department breach?

- Identify gaps in organizational identity and access management (IAM) best practices, particularly for privileged accounts. More specifically, upgrade legacy systems and deploy privileged access management (PAM) tools, adopt phishing-resistant multifactor authentication (MFA), and implement restrictions to only managed devices for high-risk access.
- Inventory all privileged accounts and increase security operations center (SOC) monitoring for abnormal behavior and for indicators of compromise, such as abnormal access volumes, unknown geographic locations, time of day access, unusual browser type and device ID.
- Perform a comprehensive audit of the IAM and SOC programs to identify policy, procedural and responsibilities gaps across the functions of configure, protect, detect, investigate and respond. In particular, ensure that preventative measures are in place to defeat known identity attacks and that SOC playbooks are adapted to rapidly investigate and respond to indicators of identity compromise.
- Use this incident to educate management and the board about the increasing risks of identity takeover attacks and to gain support and funding for the above action items.

More Detail

In April 2025, the Office of the Comptroller of the Currency (OCC) notified Congress of a major security incident. [1] The report noted that in February 2025, the OCC discovered abnormal access to U.S. Treasury Department email accounts from an authenticated administrative account. The initial OCC investigation found unauthorized access to a number of email accounts, including access to emails with highly sensitive information. While not all details of this incident have been disclosed, current public information indicates that attackers gained credentialed access to an administrative account in the email infrastructure, which gave attackers access to individual email accounts and stored email content.

This attack — along with high-profile attacks on Microsoft, MGM and other organizations in 2024 — illustrates the growing imperative for security and risk management (SRM) leaders to embark on an identity-first security project. Indeed, a recent report notes that 52% of all cybersecurity attacks have an IAM component. [2]

Identity threat detection and response (ITDR) is a discipline that includes tools and best practices that secure the IAM infrastructure from attacks. (See Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response.) ITDR includes identity posture management, which is responsible for monitoring configurations, policies and data in identity systems for indicators of exposure that can be exploited by bad actors. Identity posture management makes sure that identity systems are aligned with industry best practices such as sufficient MFA coverage, properly authorized high-risk access, prompt deactivation of unused accounts, and others.

Traditionally, IAM administration has been focused on enabling access to vital business resources, while the SOC team has been focused on real-time detection of malware, vulnerabilities and other attack paths. SRM leaders need to bring these two groups together. To get started, SRM leaders must ensure that there is a project leader with clear authority across both the IAM and SOC teams to influence priority actions and bridge the gap between the two teams.

A comprehensive audit of the IAM and SOC programs should include the following checks:

1. The IAM system is securely configured and utilizes the latest stable software version. Plans are in place to resolve IAM technical debt, bridge siloes, modernize applications and enable new use cases such as adaptive access to legacy systems.

2. IAM best practices are in place and followed by employees and administrators.

3. Phishing-resistant MFA programs are in place and adoption is measured. MFA programs should start with remote, cloud and privileged access, and increase toward all login events.

4. Proper controls are in place to prevent known attacks, such as proxy-based MFA bypass, credential stuffing attacks, MFA fatigue bombs, graymail bombs, SIM swapping and others.

5. The SOC team has the correct telemetry to detect potential credential misuse attacks.

6. The SOC team has predefined playbooks to rapidly respond to IAM attacks.

7. Analytics-based approaches such as adaptive access and continuous adaptive trust are deployed.

8. Threat intel on new IAM attack techniques are monitored for changing attacks that may necessitate defensive modifications.

9. Incident response performance metrics and tabletop exercises are developed to identify gaps in incident response playbooks.

10. Email security (antiphishing) plays a major role in protecting credentials. Ensure that credential theft phishing detection techniques and email account takeover monitoring are deployed and fully enabled. Use mail system administration monitoring capabilities to monitor logs for abnormal usage.

11. Dark web credential monitoring may be performed to determine if corporate credentials are already compromised.

While there are products that help manage and improve IAM resilience, using common top practices would likely have minimized the impact of this breach. Project managers should start with improving existing processes and fine-tuning existing security infrastructure first. We note that many organizations only leverage a fraction of the capabilities of the security and identity tools they have licensed. However, there are a number of technology solutions that project managers should consider adopting to address this type of attack:

- ITDR tools that can identify and prioritize IAM vulnerabilities as well as monitor IAM systems for suspicious events. Cisco (Oort), CrowdStrike, Microsoft, SentinelOne and Silverfort are representative vendors in this category.

- Adaptive access controls that use contextual signals (such as users' network, location and device information) to evaluate risk and perform risk-mitigating actions — for example, requiring step-up authentication (MFA), restricting access rights or blocking access altogether. Adaptive access can be extended into user sessions using emerging technologies such as the Continuous Access Evaluation Profile (CAEP) standard, and integrated with ITDR to receive additional account- and session-level risk signals (see Magic Quadrant for Access Management).

- PAM tools that provide privileged account discovery; privileged access governance and administration; privileged credential and session management; privileged access elevation and delegation; and privileged access auditing, logging and analytics. Where possible, organizations should adopt the zero standing privileges (ZSP) model granting privileged access to accounts and sessions just in time — only when needed and only for short periods of time. PAM should also include management of service accounts, which are commonly assigned administrative privileges. (See Magic Quadrant for Privileged Access Management.)

- Security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools can often be leveraged to detect suspect account takeover events via user and entity behavior analytics (UEBA) engines. (See Magic Quadrant for Security Information and Event Management.)

- Email security tools can help prevent common credential theft phishing attacks as well as monitor outbound emails to detect potentially compromised accounts. SRM leaders should investigate current antiphishing capabilities for credential theft attack defenses and account takeover detection techniques. (See Magic Quadrant for Email Security Platforms.)

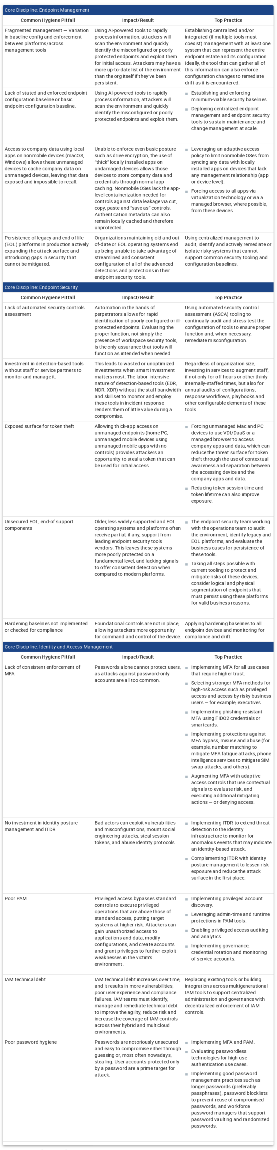
- Compromised credential monitoring services can also be helpful to identify corporate credentials that are already compromised by breaches or for sale on the dark web via credential brokers. (See How to Mitigate Account Takeover Risks.)

Of course, identity-first security is only part of an ongoing, coordinated cybersecurity program. In particular, organizations should evolve from operating security products as separate technology silos to operating them as an integrated system that shares risk signals and alerts. IAM security is not a set-it-and-forget-it task. It requires ongoing review and investment. System integrations, mergers and reorganizations can alter long-held assumptions about IAM systems and privileges. Gartner recommends assessing all components annually and including an IAM review in your organizational change toolbox. A well-coordinated cybersecurity program would also include some of the top practices described in the Appendix.

Appendix

Table 1: Common Hygiene Pitfalls and Top Practices to Mitigate

(Enlarged table in Appendix)



Core Discipline: Endpoint Management

Common Hygiene Pitfall	Impact/Result	Top Practice
Fragmented management — Variation in baseline config and enforcement between platforms/across management tools	Using AI-powered tools to rapidly process information, attackers will scan the environment and quickly identify the misconfigured or poorly protected endpoints and exploit them for initial access. Attackers may have a more up-to-date list of the environment than the org itself if they've been persistent.	Establishing centralized and/or integrated (if multiple tools must coexist) management with at least one system that can represent the entire endpoint estate and its configuration. Ideally, the tool that can gather all of this information can also enforce configuration changes to remediate drift as it is encountered.
Lack of stated and enforced endpoint configuration baseline or basic endpoint configuration baseline.	Using AI-powered tools to rapidly process information, attackers will scan the environment and quickly identify the misconfigured or poorly protected endpoints and exploit them.	■ Establishing and enforcing minimum-viable security baselines. ■ Deploying centralized endpoint management and endpoint security tools to sustain maintenance and change management at scale.
Access to company data using local apps on nonmobile devices (macOS, Windows) allows these unmanaged devices to cache company data on unmanaged devices, leaving that data exposed and impossible to recall.	Unable to enforce even basic posture such as drive encryption, the use of "thick" locally installed apps on undamaged devices allows those devices to store company data and credentials through normal app caching. Nonmobile OSes lack the app-level containerization needed for controls against data leakage via cut, copy, paste and "save as" controls. Authentication metadata can also remain locally cached and therefore unprotected.	■ Leveraging an adaptive access policy to limit nonmobile OSes from syncing any data with locally installed apps on devices that lack any management relationship (app or device level). ■ Forcing access to all apps via virtualization technology or via a managed browser, where possible, from these devices.
Persistence of legacy and end of life (EOL) platforms in production actively expanding the attack surface and introducing gaps in security that cannot be mitigated.	Organizations maintaining old and out-of-date or EOL operating systems end up being unable to take advantage of streamlined and consistent configuration of all of the advanced detections and protections in their endpoint security tools.	Using centralized management to audit, identify and actively remediate or isolate risky systems that cannot support common security tooling and configuration baselines.

Core Discipline: Endpoint Security

Common Hygiene Pitfall	Impact/Result	Top Practice
Lack of automated security controls assessment	Automation in the hands of perpetrators allows for rapid identification of poorly configured or ill-protected endpoints. Evaluating the proper function, not simply the presence of workspace security tools, is the only assurance that tools will function as intended when needed.	Using automated security control assessment (ASCA) tooling to continually audit and stress-test the configuration of tools to ensure proper function and, when necessary, remediate misconfiguration.
Investment in detection-based tools without staff or service partners to monitor and manage it.	This leads to wasted or unoptimized investments when smart investment matters most. The labor-intensive nature of detection-based tools (EDR, NDR, XDR) without the staff bandwidth and skill set to monitor and employ these tools in incident response renders them of little value during a compromise.	Regardless of organization size, investing in services to augment staff, if not only for off hours or other thinly-internally-staffed times, but also for annual audits of configurations, response workflows, playbooks and other configurable elements of these tools.
Exposed surface for token theft	Allowing thick-app access on unmanaged endpoints (home PC, unmanaged mobile devices using unmanaged mobile apps with no controls) provides attackers an opportunity to steal a token that can be used for initial access.	■ Forcing unmanaged Mac and PC devices to use VDI/DaaS or a managed browser to access company apps and data, which can reduce the threat surface for token theft through the use of contextual awareness and separation between the accessing device and the company apps and data. ■ Reducing token session time and token lifetime can also improve exposure.
Unsecured EOL, end-of support components	Older, less widely supported and EOL operating systems and platforms often receive partial, if any, support from leading endpoint security tools vendors. This leaves these systems more poorly protected on a fundamental level, and lacking signals to offer consistent detection when compared to modern platforms.	■ The endpoint security team working with the operations team to audit the environment, identify legacy and EOL platforms, and evaluate the business cases for persistence of these tools. ■ Taking all steps possible with current tooling to protect and mitigate risks of these devices; consider logical and physical segmentation of endpoints that must persist using these platforms for valid business reasons.
Hardening baselines not implemented or checked for compliance	Foundational controls are not in place, allowing attackers more opportunity for command and control of the device.	Applying hardening baselines to all endpoint devices and monitoring for compliance and drift.

Core Discipline: Identity and Access Management

Common Hygiene Pitfall	Impact/Result	Top Practice
Lack of consistent enforcement of MFA	Passwords alone cannot protect users, as attacks against password-only accounts are all too common.	■ Implementing MFA for all use cases that require higher trust. ■ Selecting stronger MFA methods for high-risk access such as privileged access and access by risky business users — for example, executives. ■ Implementing phishing-resistant MFA using FIDO2 credentials or smartcards. ■ Implementing protections against MFA bypass, misuse and abuse (for example, number matching to mitigate MFA fatigue attacks, phone intelligence services to mitigate SIM swap attacks, and others). ■ Augmenting MFA with adaptive access controls that use contextual signals to evaluate risk, and executing additional mitigating actions — or denying access.
No investment in identity posture management and ITDR	Bad actors can exploit vulnerabilities and misconfigurations, mount social engineering attacks, steal session tokens, and abuse identity protocols.	■ Implementing ITDR to extend threat detection to the identity infrastructure to monitor for anomalous events that may indicate an identity-based attack. ■ Complementing ITDR with identity posture management to lessen risk exposure and reduce the attack surface in the first place.
Poor PAM	Privileged access bypasses standard controls to execute privileged operations that are above those of standard access, putting target systems at higher risk. Attackers can gain unauthorized access to applications and data, modify configurations, and create accounts and grant privileges to further exploit weaknesses in the victim's environment.	■ Implementing privileged account discovery. ■ Leveraging admin-time and runtime protections in PAM tools. ■ Enabling privileged access auditing and analytics. ■ Implementing governance, credential rotation and monitoring of service accounts.
IAM technical debt	IAM technical debt increases over time, and it results in more vulnerabilities, poor user experience and compliance failures. IAM teams must identify, manage and remediate technical debt to improve the agility, reduce risk and increase the coverage of IAM controls across their hybrid and multicloud environments.	Replacing existing tools or building integrations across multigenerational IAM tools to support centralized administration and governance with decentralized enforcement of IAM controls.
Poor password hygiene	Passwords are notoriously unsecured and easy to compromise either through guessing or, most often nowadays, stealing. User accounts protected only by a password are a prime target for attack.	■ Implementing MFA and PAM. ■ Evaluating passwordless technologies for high-use authentication use cases. ■ Implementing good password management practices such as longer passwords (preferably passphrases), password blocklists to prevent reuse of compromised passwords, and workforce password managers that support password vaulting and randomized passwords.

Source: Gartner (April 2025)

Contributors

Eric Grenier, Paul Rabinovich, Mary Ruddy, Chris Silva, Erik Wahlstrom

Evidence

[1] OCC Notifies Congress of Incident Involving Email System, Office of the Comptroller of the Currency.

[2] CrowdStrike 2025 Global Threat Report, CrowdStrike.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

A Journey Guide to Building a Security Operations Center

Choose the Right Tools in Your Security Operations Maturity Journey

Reduce IAM Technical Debt

Address Top IAM Hygiene Issues to Enhance Security and Reduce Risk

Prioritize IAM Hygiene for Robust Identity-First Security

Table 1: Common Hygiene Pitfalls and Top Practices to Mitigate

Core Discipline: Endpoint Management		
Common Hygiene Pitfall	**Impact/Result**	**Top Practice**
Fragmented management — Variation in baseline config and enforcement between platforms/across management tools	Using AI-powered tools to rapidly process information, attackers will scan the environment and quickly identify the misconfigured or poorly protected endpoints and exploit them for initial access. Attackers may have a more up-to-date list of the environment than the org itself if they've been persistent.	Establishing centralized and/or integrated (if multiple tools must coexist) management with at least one system that can represent the entire endpoint estate and its configuration. Ideally, the tool that can gather all of this information can also enforce configuration changes to remediate drift as it is encountered.
Lack of stated and enforced endpoint configuration baseline or basic endpoint configuration baseline.	Using AI-powered tools to rapidly process information, attackers will scan the environment and quickly identify the misconfigured or poorly protected endpoints and exploit them.	▪ Establishing and enforcing minimum-viable security baselines. ▪ Deploying centralized endpoint management and endpoint security tools to sustain maintenance and change management at scale.
Access to company data using local apps on nonmobile devices (macOS, Windows) allows these unmanaged devices to cache company data on unmanaged devices, leaving that data exposed and impossible to recall.	Unable to enforce even basic posture such as drive encryption, the use of "thick" locally installed apps on undamaged devices allows those devices to store company data and credentials through normal app caching. Nonmobile OSes lack the app-level containerization needed for controls against data leakage via cut, copy, paste and "save as"	▪ Leveraging an adaptive access policy to limit nonmobile OSes from syncing any data with locally installed apps on devices that lack any management relationship (app or device level). ▪ Forcing access to all apps via virtualization technology or via a managed browser, where

	controls. Authentication metadata can also remain locally cached and therefore unprotected.	possible, from these devices.
Persistence of legacy and end of life (EOL) platforms in production actively expanding the attack surface and introducing gaps in security that cannot be mitigated.	Organizations maintaining old and out-of-date or EOL operating systems end up being unable to take advantage of streamlined and consistent configuration of all of the advanced detections and protections in their endpoint security tools.	Using centralized management to audit, identify and actively remediate or isolate risky systems that cannot support common security tooling and configuration baselines.
Core Discipline: Endpoint Security		
Common Hygiene Pitfall	**Impact/Result**	**Top Practice**
Lack of automated security controls assessment	Automation in the hands of perpetrators allows for rapid identification of poorly configured or ill-protected endpoints. Evaluating the proper function, not simply the presence of workspace security tools, is the only assurance that tools will function as intended when needed.	Using automated security control assessment (ASCA) tooling to continually audit and stress-test the configuration of tools to ensure proper function and, when necessary, remediate misconfiguration.
Investment in detection-based tools without staff or service partners to monitor and manage it.	This leads to wasted or unoptimized investments when smart investment matters most. The labor-intensive nature of detection-based tools (EDR, NDR, XDR) without the staff bandwidth and skill set to monitor and employ these tools in incident response renders them of little value during a compromise.	Regardless of organization size, investing in services to augment staff, if not only for off hours or other thinly-internally-staffed times, but also for annual audits of configurations, response workflows, playbooks and other configurable elements of these tools.
Exposed surface for token theft	Allowing thick-app access on unmanaged endpoints (home PC, unmanaged mobile devices	■ Forcing unmanaged Mac and PC devices to use VDI/DaaS or a managed browser to access

	using unmanaged mobile apps with no controls) provides attackers an opportunity to steal a token that can be used for initial access.	company apps and data, which can reduce the threat surface for token theft through the use of contextual awareness and separation between the accessing device and the company apps and data. ▪ Reducing token session time and token lifetime can also improve exposure.
Unsecured EOL, end-of support components	Older, less widely supported and EOL operating systems and platforms often receive partial, if any, support from leading endpoint security tools vendors. This leaves these systems more poorly protected on a fundamental level, and lacking signals to offer consistent detection when compared to modern platforms.	▪ The endpoint security team working with the operations team to audit the environment, identify legacy and EOL platforms, and evaluate the business cases for persistence of these tools. ▪ Taking all steps possible with current tooling to protect and mitigate risks of these devices; consider logical and physical segmentation of endpoints that must persist using these platforms for valid business reasons.
Hardening baselines not implemented or checked for compliance	Foundational controls are not in place, allowing attackers more opportunity for command and control of the device.	Applying hardening baselines to all endpoint devices and monitoring for compliance and drift.
Core Discipline: Identity and Access Management		
Common Hygiene Pitfall	**Impact/Result**	**Top Practice**

Lack of consistent enforcement of MFA	Passwords alone cannot protect users, as attacks against password-only accounts are all too common.	■ Implementing MFA for all use cases that require higher trust. ■ Selecting stronger MFA methods for high-risk access such as privileged access and access by risky business users — for example, executives. ■ Implementing phishing-resistant MFA using FIDO2 credentials or smartcards. ■ Implementing protections against MFA bypass, misuse and abuse (for example, number matching to mitigate MFA fatigue attacks, phone intelligence services to mitigate SIM swap attacks, and others). ■ Augmenting MFA with adaptive access controls that use contextual signals to evaluate risk, and executing additional mitigating actions — or denying access.
No investment in identity posture management and ITDR	Bad actors can exploit vulnerabilities and misconfigurations, mount social engineering attacks, steal session tokens, and abuse identity protocols.	■ Implementing ITDR to extend threat detection to the identity infrastructure to monitor for anomalous events that may indicate an identity-based attack. ■ Complementing ITDR with identity posture management to lessen risk exposure and reduce the attack surface in the first place.

Poor PAM	Privileged access bypasses standard controls to execute privileged operations that are above those of standard access, putting target systems at higher risk. Attackers can gain unauthorized access to applications and data, modify configurations, and create accounts and grant privileges to further exploit weaknesses in the victim's environment.	▪ Implementing privileged account discovery. ▪ Leveraging admin-time and runtime protections in PAM tools. ▪ Enabling privileged access auditing and analytics. ▪ Implementing governance, credential rotation and monitoring of service accounts.
IAM technical debt	IAM technical debt increases over time, and it results in more vulnerabilities, poor user experience and compliance failures. IAM teams must identify, manage and remediate technical debt to improve the agility, reduce risk and increase the coverage of IAM controls across their hybrid and multicloud environments.	Replacing existing tools or building integrations across multigenerational IAM tools to support centralized administration and governance with decentralized enforcement of IAM controls.
Poor password hygiene	Passwords are notoriously unsecured and easy to compromise either through guessing or, most often nowadays, stealing. User accounts protected only by a password are a prime target for attack.	▪ Implementing MFA and PAM. ▪ Evaluating passwordless technologies for high-use authentication use cases. ▪ Implementing good password management practices such as longer passwords (preferably passphrases), password blocklists to prevent reuse of compromised passwords, and

	workforce password managers that support password vaulting and randomized passwords.

Source: Gartner (April 2025)