Product ID: AA22-131A

May 11, 2022

Co-authored by:

National Cyber Security Centre a part of GCHQ
ACSC Australian Cyber Security Centre
Communications Security Establishment Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité
GOVERNMENT COMMUNICATIONS SECURITY BUREAU TE TIRA TIAKI

Protecting Against Cyber Threats to Managed Service Providers and their Customers

SUMMARY

The cybersecurity authorities of the United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), and the United States (CISA), (NSA), (FBI) are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue.[1] This joint Cybersecurity Advisory (CSA) provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber intrusion.

This advisory describes cybersecurity best practices for information and communications technology (ICT) services and functions, focusing on guidance that enables transparent discussions between MSPs and their customers on securing sensitive data. Organizations should implement these guidelines as appropriate to their unique environments, in accordance with their specific security needs, and in compliance with applicable regulations. MSP customers should verify that the contractual arrangements with their provider include cybersecurity measures in line with their particular security requirements.

Tactical actions for MSPs and their customers to take today:

- Identify and disable accounts that are no longer in use.
- Enforce MFA on MSP accounts that access the customer environment and monitor for unexplained failed authentication.
- Ensure MSP-customer contracts transparently identify ownership of ICT security roles and responsibilities.

The guidance provided in this advisory is specifically tailored for both MSPs and their customers and is the result of a collaborative effort from the United Kingdom National Cyber Security Centre (NCSC-UK), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), the United States' Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) with contributions from industry members of the Joint Cyber Defense Collaborative

(JCDC). Organizations should read this advisory in conjunction with NCSC-UK guidance on actions to take when the cyber threat is heightened , CCCS guidance on Cyber Security Considerations for Consumers of Managed Services, and CISA guidance provided on the Shields Up and Shields Up Technical Guidance webpages.

Managed Service Providers

This advisory defines MSPs as entities that deliver, operate, or manage ICT services and functions for their customers via a contractual arrangement, such as a service level agreement. In addition to offering their own services, an MSP may offer services in conjunction with those of other providers. Offerings may include platform, software, and IT infrastructure services; business process and support functions; and cybersecurity services. MSPs typically manage these services and functions in their customer's network environment—either on the customer's premises or hosted in the MSP's data center. **Note:** this advisory does not address guidance on cloud service providers (CSPs)—providers who handle the ICT needs of their customers via cloud services such as Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service; however, MSPs may offer these services as well. (See Appendix for additional definitions.)

MSPs provide services that usually require both trusted network connectivity and privileged access to and from customer systems. Many organizations—ranging from large critical infrastructure organizations to small- and mid-sized businesses—use MSPs to manage ICT systems, store data, or support sensitive processes. Many organizations make use of MSPs to scale and support network environments and processes without expanding their internal staff or having to develop the capabilities internally.

Threat Actors Targeting MSP Access to Customer Networks

Whether the customer's network environment is on premises or externally hosted, threat actors can use a vulnerable MSP as an initial access vector to multiple victim networks, with globally cascading effects. The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities expect malicious cyber actors—including state-sponsored advanced persistent threat (APT) groups—to step up their targeting of MSPs in their efforts to exploit provider-customer network trust relationships. For example, threat actors successfully compromising an MSP could enable follow-on activity—such as ransomware and cyber espionage—against the MSP as well as across the MSP's customer base.

The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities have previously issued general guidance for MSPs and their customers.[2],[3],[4],[5],[6],[7],[8] This advisory provides specific guidance to enable transparent, well-informed discussions between MSPs and their customers that center on securing sensitive information and data. These discussions should result in a re-evaluation of security processes and contractual commitments to accommodate customer risk tolerance. A shared commitment to security will reduce risk for both MSPs and their customers, as well as the global ICT community.

RECOMMENDATIONS

MSPs and their Customers

The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities recommend MSPs and their customers implement the baseline security measures and operational controls listed in this

section. Additionally, customers should ensure their contractual arrangements specify that their MSP implements these measures and controls.

Prevent initial compromise.

In their efforts to compromise MSPs, malicious cyber actors exploit vulnerable devices and internet-facing services, conduct brute force attacks, and use phishing techniques. MSPs and their customers should ensure they are mitigating these attack methods. Useful mitigation resources on initial compromise attack methods are listed below:

- Improve security of vulnerable devices.
  - Selecting and Hardening Remote Access VPN Solutions (CISA, NSA)
  - Vulnerability Scanning Tools and Services (NCSC-UK)
- Protect internet-facing services.
  - Protecting internet-facing services on public service Critical National Infrastructure (CNI) (NCSC-UK)
  - Strategies for protecting web application systems against credential stuffing attacks (CCCS)
- Defend against brute force and password spraying.
  - Microsoft update on brute force and password spraying activity (NCSC-UK)
  - Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments (NSA, CISA, FBI, NCSC-UK)
- Defend against phishing.
  - Phishing attacks: defending your organisation (NCSC-UK)
  - Spotting malicious email messages (CCCS)

Enable/improve monitoring and logging processes.

It can be months before incidents are detected, so UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities recommend all organizations store their most important logs for at least six months. Whether through a comprehensive security information and event management (SIEM) solution or discrete logging tools, implement and maintain a segregated logging regime to detect threats to networks. Organizations can refer to the following NCSC-UK guidance on the appropriate data to collect for security purposes and when to use it: What exactly should we be logging?. Additionally, all organizations—whether through contractual arrangements with an MSP or on their own—should implement endpoint detection and network defense monitoring capabilities in addition to using application allowlisting/denylisting.

- **MSPs** should log the delivery infrastructure activities used to provide services to the customer. MSPs should also log both internal and customer network activity, as appropriate and contractually agreed upon**.**
- **Customers** should enable effective monitoring and logging of their systems. If customers choose to engage an MSP to perform monitoring and logging, they should ensure that their contractual arrangements require their MSP to:
  - Implement comprehensive security event management that enables appropriate monitoring and logging of provider-managed customer systems;
  - Provide visibility—as specified in the contractual arrangement—to customers of logging activities, including provider's presence, activities, and connections to the

customer networks (**Note:** customers should ensure that MSP accounts are properly monitored and audited.); and
    - Notify customer of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks, and send these to a security operations center (SOC) for analysis and triage.

Enforce multifactor authentication (MFA).

Organizations should secure remote access applications and enforce MFA where possible to harden the infrastructure that enables access to networks and systems.[9],[10] **Note:** Russian state-sponsored APT actors have recently demonstrated the ability to exploit default MFA protocols; organizations should review configuration policies to protect against "fail open" and re-enrollment scenarios.[11]

- **MSPs** should recommend the adoption of MFA across all customer services and products. **Note:** MSPs should also implement MFA on all accounts that have access to customer environments and should treat those accounts as privileged.
- **Customers** should ensure that their contractual arrangements mandate the use of MFA on the services and products they receive. Contracts should also require MFA to be enforced on all MSP accounts used to access customer environments.

Manage internal architecture risks and segregate internal networks.

Organizations should understand their environment and segregate their networks. Identify, group, and isolate critical business systems and apply appropriate network security controls to them to reduce the impact of a compromise across the organization.[12],[13]

- **MSPs** should review and verify all connections between internal systems, customer systems, and other networks. Segregate customer data sets (and services, where applicable) from each other—as well as from internal company networks—to limit the impact of a single vector of attack. Do not reuse admin credentials across multiple customers.
- **Customers** should review and verify all connections between internal systems, MSP systems, and other networks. Ensure management of identity providers and trusts between the different environments. Use a dedicated virtual private network (VPN) or alternative secure access method, to connect to MSP infrastructure and limit all network traffic to and from the MSP to that dedicated secure connection. Verify that the networks used for trust relationships with MSPs are suitably segregated from the rest of their networks. Ensure contractual agreements specify that MSPs will not reuse admin credentials across multiple customers.

Apply the principle of least privilege.

Organizations should apply the principle of least privilege throughout their network environment and immediate update privileges upon changes in administrative roles. Use a tiering model for administrative accounts so that these accounts do not have any unnecessary access or privileges. Only use accounts with full privileges across an enterprise when strictly necessary and consider the use of time-based privileges to further restrict their use. Identify high-risk devices, services and users to minimize their accesses.[14]

- **MSPs** should apply this principle to both internal and customer environments, avoiding default administrative privileges.

- **Customers** should ensure that their MSP applies this principle to both provider and customer network environments. **Note:** customers with contractual arrangements that provide them with administration of MSP accounts within their environment should ensure that the MSP accounts only have access to the services/resources being managed by the MSP.

Deprecate obsolete accounts and infrastructure.

Both MSPs and customers should periodically review their internet attack surface and take steps to limit it, such as disabling user accounts when personnel transition.[15] (**Note:** although sharing accounts is not recommended, should an organization require this, passwords to shared account should be reset when personnel transition.) Organizations should also audit their network infrastructure—paying particular attention to those on the MSP-customer boundary—to identify and disable unused systems and services. Port scanning tools and automated system inventories can assist organizations in confirming the roles and responsibilities of systems.

- **Customers** should be sure to disable MSP accounts that are no longer managing infrastructure. **Note:** disabling MSP accounts can be overlooked when a contract terminates.

Apply updates.

Organizations should update software, including operating systems, applications, and firmware. Prioritize applying security updates to software containing known exploited vulnerabilities. **Note:** organizations should prioritize patching vulnerabilities included in CISA's catalogue of known exploited vulnerabilities (KEV) as opposed to only those with high Common Vulnerability Scoring System (CVSS) scores that have not been exploited and may never be exploited.[16],[17],[18],[19]

- **MSPs** should implement updates on internal networks as quickly as possible.
- **Customers** should ensure that they understand their MSP's policy on software updates and request that comprehensive and timely updates are delivered as an ongoing service.

Backup systems and data.

Organizations should regularly update and test backups—including "gold images" of critical systems in the event these need to be rebuilt (**Note:** organizations should base the frequency of backups on their recovery point objective [20]). Store backups separately and isolate them from network connections that could enable the spread of ransomware; many ransomware variants attempt to find and encrypt/delete accessible backups. Isolating backups enables restoration of systems/data to their previous state should they be encrypted with ransomware. **Note:** best practices include storing backups separately, such as on external media.[21],[22],[23]

- **MSPs** should regularly backup internal data as well as customer data (where contractually appropriate) and maintain offline backups encrypted with separate, offline encryption keys. Providers should encourage customers to create secure, offsite backups and exercise recovery capabilities.
- **Customers** should ensure that their contractual arrangements include backup services that meet their resilience and disaster recovery requirements. Specifically, customers should require their MSP to implement a backup solution that automatically and continuously backs up critical data and system configurations and store backups in an easily retrievable location, e.g., a cloud-based solution or a location that is air-gapped from the organizational network.

Develop and exercise incident response and recovery plans.

Incident response and recovery plans should include roles and responsibilities for all organizational stakeholders, including executives, technical leads, and procurement officers. Organizations should maintain up-to-date hard copies of plans to ensure responders can access them should the network be inaccessible (e.g., due to a ransomware attack).[24]

- **MSPs** should develop and regularly exercise internal incident response and recovery plans and encourage customers to do the same.
- **Customers** should ensure that their contractual arrangements include incident response and recovery plans that meet their resilience and disaster recovery requirements. Customers should ensure these plans are tested at regular intervals.

Understand and proactively manage supply chain risk.

All organizations should proactively manage ICT supply chain risk across security, legal, and procurement groups, using risk assessments to identify and prioritize the allocation of resources.[25],[26]

- **MSPs** should understand their own supply chain risk and manage the cascading risks it poses to customers.
- **Customers** should understand the supply chain risk associated with their MSP, including risk associated with third-party vendors or subcontractors. Customers should also set clear network security expectations with their MSPs and understand the access their MSP has to their network and the data it houses. Each customer should ensure their contractual arrangements meet their specific security requirements and that their contract specifies whether the MSP or the customer owns specific responsibilities, such as hardening, detection, and incident response.[27]

Promote transparency.

Both MSPs and their customers will benefit from contractual arrangements that clearly define responsibilities.

- **MSPs,** when negotiating the terms of a contract with their customer, should provide clear explanations of the services the customer is purchasing, services the customer is not purchasing, and all contingencies for incident response and recovery.
- **Customers** should ensure that they have a thorough understanding of the security services their MSP is providing via the contractual arrangement and address any security requirements that fall outside the scope of the contract. **Note:** contracts should detail how and when MSPs notify the customer of an incident affecting the customer's environment.

Manage account authentication and authorization.

All organizations should adhere to best practices for password and permission management. [28],[29],[30] Organizations should review logs for unexplained failed authentication attempts—failed authentication attempts directly following an account password change could indicate that the account had been compromised. **Note:** network defenders can proactively search for such "intrusion canaries" by reviewing logs after performing password changes—using off-network communications to inform users of the changes—across all sensitive accounts. (See the ACSC publication, Windows Event

Logging and Forwarding as well as Microsoft's documentation, 4625(F): An account failed to log on . for additional guidance.)

- **MSPs** should verify that the customer restricts MSP account access to systems managed by the MSP.
- **Customers** should ensure MSP accounts are not assigned to internal administrator groups; instead, restrict MSP accounts to systems managed by the MSP. Grant access and administrative permissions on a need-to-know basis, using the principle of least privilege. Verify, via audits, that MSP accounts are being used for appropriate purposes and activities, and that these accounts are disabled when not actively being used.

PURPOSE

This advisory was developed by UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities in furtherance their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

ACKNOWLEDGEMENTS

The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities would like to acknowledge Secureworks for their contributions to this CSA.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. NCSC-UK, ACSC, CCCS, NCSC-NZ, CISA, NSA, and FBI do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favouring.

CONTACT INFORMATION

United Kingdom organizations: report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973. **Australian organizations:** visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories. **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca. **New Zealand organizations:** report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654. **U.S. organizations:** all organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI’s 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

RESOURCES

In addition to the guidance referenced above, see the following resources:

- Joint CSA: Technical Approaches to Uncovering and Remediating Malicious Activity
- Joint CSA: 2021 Trends Show Increased Globalized Threat of Ransomware
- ACSC's Managed Service Providers: How to manage risk to customer networks
- CCCS:
  - Cyber Security Considerations for Consumers of Managed Services
  - Baseline Cyber Security Controls for Small and Medium Organizations
  - Top 10 IT Security Action Items to Protect Internet Connected Networks and Information
  - CCCS's Alert: Malicious Cyber Activity Targeting Managed Service Providers
- CISA:
  - CISA Cybersecurity Alert: APT Activity Exploiting MSPs (2018)
  - CISA Cyber Essentials and CISA Cyber Resource Hub
- FBI Internet Crime Complaint Center alerts on malicious and criminal cyber activity
- National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE): Improving Cybersecurity of Managed Service Providers

REFERENCES

[1] State of the Market: The New Threat Landscape, Pushing MSP security to the next level (N-able)

[2] Global targeting of enterprises via managed service providers (NCSC-UK)

[3] Guidance for MSPs and Small- and Mid-sized Businesses (CISA)

[4] Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers (CISA)

[5] APTs Targeting IT Service Provider Customers (CISA)

[6] MSP Investigation Report (ACSC)

[7] How to Manage Your Security When Engaging a Managed Service Provider

[8] Supply Chain Cyber Security: In Safe Hands (NCSC-NZ)

[9] Multi-factor authentication for online services (NCSC-UK)

[10] Zero trust architecture design principles: MFA (NCSC-UK)

[11] Joint CISA-FBI CSA: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default MFA Protocols and “PrintNightmare” Vulnerability

[12] Security architecture anti-patterns (NCSC-UK)

[13] Preventing Lateral Movement (NCSC-UK)

[14] Preventing Lateral Movement: Apply the principle of least privilege (NCSC-UK)

[15] Device Security Guidance: Obsolete products (NCSC-UK)

[16] Known Exploited Vulnerabilities Catalog (CISA)

[17] The problems with patching (NCSC-UK)

[18] Security principles for cross domain solutions: Patching (NCSC-UK)

[19] Joint CSA: 2021 Top Routinely Exploited Vulnerabilities

[20] Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files (NIST)

[21] Stop Ransomware website (CISA)

[22] Offline backups in an online world (NCSC-UK)

[23] Mitigating malware and ransomware attacks (NCSC-UK)

[24] Effective steps to cyber exercise creation (NCSC-UK)

[25] Supply chain security guidance (NCSC-UK)

[26] ICT Supply Chain Resource Library (CISA)

[27] Risk Considerations for Managed Service Provider Customers (CISA)

[28] Device Security Guidance: Enterprise authentication policy (NCSC-UK)

[29] Preventing Lateral Movement: Apply the principle of least privilege (NCSC-UK)

[30] Implementing Strong Authentication (CISA)

APPENDIX

This advisory's definition of MSPs aligns with the following definitions.

The definition of MSP from Gartner's Information Technology Glossary—which is also referenced by NIST in the Improving Cybersecurity of Managed Service Providers—is:

> *A managed service provider (MSP) delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data center (hosting), or in a third-party data center.*
>
> *MSPs may deliver their own native services in conjunction with other providers' services (for example, a security MSP providing sys admin on top of a third-party cloud IaaS). Pure-play MSPs focus on one vendor or technology, usually their own core offerings. Many MSPs include services from other types of providers. The term MSP traditionally was applied to infrastructure or device-centric types of services but has expanded to include any continuous, regular management, maintenance and support.*

The United Kingdom's Department of Digital, Culture, Media, and Sport (DCMS) recently published the following definition of MSP, which includes examples:

> *Managed Service Provider - A supplier that delivers a portfolio of IT services to business customers via ongoing support and active administration, all of which are typically underpinned by a Service Level Agreement. A Managed Service Provider may provide their own Managed Services or offer their own services in conjunction with other IT providers' services. The Managed Services might include:*
>
> - *Cloud computing services (resale of cloud services, or an in-house public and private cloud services, built and provided by the Managed Service Providers)*
> - *Workplace services*
> - *Managed Network*
> - *Consulting*
> - *Security services*
> - *Outsourcing*
> - *Service Integration and Management*
> - *Software Resale*
> - *Software Engineering*
> - *Analytics and Artificial Intelligence (AI)*
> - *Business Continuity and Disaster Recovery services*
>
> *The Managed Services might be delivered from customer premises, from customer data centres, from Managed Service Providers' own data centres or from 3rd party facilities (co-location facilities, public cloud data centres or network Points of Presence (PoPs)).*