Lessons Learned from NASA

How to Operate in a Compromised Environment

Trusted Recovery from the SolarWinds Breach

Jerry L. Davis, MSc.
Founder, Gryphon X, LLC
January | 2021

GRYPHON X
TRANSFORMATIVE CYBER

What this is and what it is not

This is an information sharing effort, based off my experiences and lessons learned. This is not gospel. It is not endorsed by NASA, the CIA, the Marine Corps, the cybersecurity community, any homeowner's association, or Internet Fashinova influencers. There are no "Like" or "Not Like" buttons. There is no TickTok video that accompanies this document.

I recognize that a lot of great information is being provided by community experts on how best to mitigate the impact of the SolarWinds compromise that took place in December of 2020, AKA "The year of the great dumpster fire". While triage and mitigation are the top priorities, the processes of transitioning a compromised environment back to a known good state is not trivial, especially given the wide and deep nature of this particular breach and the bad actors involved. This is not a dig at the folks at SolarWinds. It is also not a dig at the folks at NASA. For anyone that has done it in the past, defending an organization against nation state sponsored attacks is harrowing and ridiculously hard.

What I have not seen thus far is information on how to successfully operate while the environment is in a state of compromise. This document is my cheeky guidance on how to do just that; operate in a compromised environment. Better yet, the guidance laid out herein is not regulated for use specific only to the SolarWinds compromise. This guidance can be used for *any* cybersecurity compromise. It can also serve as a companion to one's established incident response processes and procedures.

I have been fortunate enough to spend a large portion of my career defending organizations against Advance Persistent Threats, combining my skills as a cyber and technology risk executive and as a counterintelligence officer. I have combined all of that experience in a vignette style case study with the guidance at the end.

While I am being cheeky in prose, I take this compromise very serious. I cannot reiterate this point strongly enough. When I view this entire campaign from my counterintelligence lenses, I have grave concern. We are vulnerable and exposed and severely wounded.

I believe that the information contained within is helpful and that the reader will extract a little bit of comic relief along the way.

Stay in the fight….

P.S. Yes, I have seen the alien spacecrafts in the basement, and yeah, I could tell you where they are, but then I'd have to…

My two cents on the SolarWinds compromise: The "twofer"

I spent the early years of my career in the intelligence community. To be exact, the counterintelligence field, first as a Marine Counterintelligence Specialist and later as a Central Intelligence Agency (CIA) Counterintelligence Officer. The work of intelligence was once famously described as "a wilderness of mirrors" by James Jesus Angleton, the career CIA officer who recast and led the CIA's Counterintelligence (CI) capabilities during the Cold War. In my mind, if intelligence work is a wilderness of mirrors, then CI work is all about being an expert at observing and identifying which of the images are mirrored reflections, which are the real persons, and more importantly, what is their purpose for being in the wilderness. CI work is one-part science, three-parts art, and a generous amount of intuition, punctuated by dashes of serendipity. Being a CI officer means understanding, in great detail, how clandestine tradecraft works and how it is employed, and for what purpose. A good CI officer can put all of these tactics and techniques together and produce an accurate estimate of what the adversary intentions are and orchestrate and execute a plan to thwart the adversary's operations.

The SolarWinds compromise looks very familiar to me. In my experience, the compromise has all the markings of a classical intelligence gathering campaign in support of preemptive *future offensive or defensive actions,* political or otherwise by a nation state sponsored adversary. The SolarWinds compromise is what I would call a "twofer". A twofer provides the adversary with at least two very strategic advantages for the price of one compromise. This first advantage is derived from the gathering and analysis of compromised data and information for intelligence analysis. Imagine what a nation state government could learn by having unfettered access to the national and international strategic theses of the US Treasury, State, Energy, Commerce, Health and Human Services, Justice, and Defense departments as examples. This advantage is a political advantage that could be used to disrupt our economy, erode our military defensive posture, and gain critical geopolitical benefits well ahead of our country.

Now imagine on the other hand, the adversary leveraging persistent access to these compromised environments while having the capability to disrupt, degrade, destroy, or cause for the loss of confidence in data, information or the systems that process, store, or transmit it preemptively and at their leisure. This is the risk proposition that is the hardest to balance because the will and intent of the adversary is unknown.

My experience at NASA and our difficulties in mitigating the impact of the Titan Rain campaign in the mid-2000 timeframe is what makes the SolarWinds compromise seem so familiar. Not familiar in attack type, but the purpose of the attack and the twofer concept.

In the case study that follows, understand that at NASA we were engaged in a multi-year cyber-Judo tournament with a very persistent and skillful adversary. Initially it appeared that the bad actors only wanted to get their hands on anything that they could and run-off. Like a juvenile "smash and grab" type of petty crime. But in understanding the type and amount of data that was

being harvested and the various pivots and lateral movements throughout the network demonstrated to me that this was a more strategic activity, and a "twofer" was in the making.

The Titan Rain bad actors sought space domain related sensitive data and information as a way to advance their own space initiatives, which by 2010, had grown out of the embryonic stage, but was still fairly infantile and not remotely on par with the US and other leading nations' space programs. However, if one immersed themselves in the strategic plans of the Titan Rain adversary, one could readily identify that their belligerent philandering inside NASA's networks consistently and accurately reconciled with their published, strategic military and space dominance goals to assert and project power; demonstrating the weaponization of Computer Network Exploitation (CNE) as an access and disruptive capability.

I would opine that the adversary's data gathering and analysis activities starting in 2006, as it related to NASA, culminated several years later into useful intelligence and insight that then led to the purposeful interference of two earth observing and imaging space platforms. Furthermore, I believe that this display of interference was purposeful and a token demonstration to show the strength of their CNE capabilities and that their position as a nation with a viable counterspace program must be respected. My roots as an intelligence officer led me to the realization that this particular adversary could mortally wound us, at will, if the desire and intent manifested.

Someone is screwing with our satellites

If memory serves me correct, it was mid-summer, 2009 when "Porter" (names have been changed to protect the innocent), launched himself into my office with a bundle of papers in his hands. What I distinctly remember was the look on his face; concern and bewilderment. This struck me as odd because Porter, whom I have had many interactions with up until that point, was always a fairly calm, collected, and cerebral individual. He had come from an Air Force background and was an engineer of "some type". What his job entailed was a mystery to me, all I knew was that he was generally in attendance whenever there was a cyber focused classified briefing inside the main secure facility located in the HQ building. Porter never really said much in those briefings, for the most part he tucked himself away quietly in the dark corners of the room (I never witnessed him enter or leave, I think he just shapeshifted into the walls). What I did know about him did not amount to much other than he freelanced around on behalf of NASA's Office of the Chief Engineer and worked on "special projects" (yeah, those type of real *special* projects).

Porter, with bundle in hand, hurriedly made his way over to the side of my desk, opened the bundle of paper, which amounted to the length of a sales receipt one gets from CVS after a purchase, and started the conversations of all conversations. What he had in hand would eventually make its way to the highest levels of the Whitehouse and to a number of Congressional members who served on the Senate Select Committee on Intelligence. Several years later, the story that follows would also become a featured Bloomberg article based on the account of the space asset interference being published in the November *2011 Report to Congress of the U.S.-China Economic and Security Review Commission*.

As Porter unraveled the Dead Sea Scrolls, I could immediately see that I was in for a long year. On the paper was a graphical printout of a bunch of squiggly (excuse the overly technical term) lines that looked like a polygraph result in which someone (me??) had failed miserably. Unfortunately, I was not that lucky as Porter described to me that this was a snapshot of the telemetry, tracking and control (TTC) printout of a signal sent to Landsat 7, a satellite used for collecting Earth based imagery. The problem was, as Porter relayed to me, was that the signal that was transmitted to Landsat 7 was not initiated by any personnel managing one of the many ground stations needed to communicate with and control the satellite.

What added color to the event was the revelation that this was not the only time that this had taken place. Porter showed me elsewhere in the printout that another Earth Observing platform, Terra-AM 1, had been interfered with as well. Just when I did not think it could get much worse, it did. There were *multiple* instances of interferences to these combined billion-dollars-plus space assets. Landsat 7 had been interfered with in October of 2007 and again in July of 2008. Terra-AM 1 had witness interference in June of 2008 and then in October of that same year. Porter explained to me thatt the unknowns who initiated the interference was able to get each platform to acknowledge that it was ready to receive commands. Thankfully, no commands were ever issued by the unknowns. It was as if they wanted us to know they were there and could take over the platforms if they chose to do so.

With my pucker factor on high, I immediately initiated a series of actions to rule out a cyber compromise of a portion of the infrastructure that was used to manage TTC. After several weeks of investigatory activities, the team could not find any instance of compromise at that particular location. By then, the whole issue was out of my hands and conversations between the Whitehouse, Department of Defense officials, and NASA's top-level leadership were well under way and I never heard another thing about the entire episode (until the Bloomberg article in 2011).

Advanced persistent pain in the neck

I had arrived at NASA in September of 2007, so I guess the whole Landsat 7 and Terra-AM 1 was my belated new Chief Information Security Officer (CISO) "hazing" launch party thrown by a hostile organization who wanted to welcome me to the space club in a dramatic fashion (mission accomplished). However this was not the first time I had interactions with the Titan Rain intrusion set since my arrival, but it was by far the most enlightening. Within my first few days at NASA, I was indoctrinated and briefed in the secure facility by NASA's counterintelligence apparatus on an ongoing, years-long activity to identify and rid NASA's networks from a nation state sponsored bad actor (an Advanced Persistent Threat or APT). NASA, for obvious reasons, was and is one of the most highly, if not most targeted organization in the federal government by bad actors of every ilk. The constant and unrelenting barrage of compromises enacted by these bad actors forced every concerned entity within NASA to spend hours to months in support of triage efforts in what I was now cursing under my breath and calling "The Advanced Persistent Pain in the Neck" (I didn't use the word "neck", but you understand.). This was on top of dealing with all the script kiddie attacks, hacktivists,

reconciling billions of hostile port scans, and non-malicious insiders engaging in stupid pet tricks that often resulted in network compromises or security policy violation.

Briefing NASA's top-level leadership on bad news was becoming routine and lulled some into a position of complacency because it was the same story every month; I never had good news to bring to the briefings. It was not for a lack of effort; we were losing a battle to determined actors, with an impressive tool bag, backed by the government of a foreign nation. They were skilled, persistent, and absurdly annoying. I had the sense that they knew our network infrastructure better than we and that left me feeling out-manned and out-gunned. I often wanted to throw my lollipop in the dirt, pickup my football and go home. Because I was a federal senior executive, a cybersecurity professional, and a Marine, the thought of quitting was never a viable option (que up Marine Corps hymn music).

Part of NASA's strategic response was to consolidate the security operations of its ten major Centers into a single and global Security Operations Center (SOC). This would provide detailed visibility into cross domain network communications and technology resources, along with the implementation of consistent security practices and procedures all culminating into a "Common Cyber Operating Picture". Putting it all together was hard. Really hard, and it took every bit of my three years as the agency's starting cybersecurity quarterback to move the football sufficiently enough downfield to where I felt comfortable declaring some measure of success.

Despite all the work that many across NASA did to improve the environment and despite our ridiculous stack of security technology we purchased and deployed, we still had enormous challenges in fending off the most sophisticated bad actors. Even with greater visibility into what was taking place on our network and with our technology resources, we determined that we still had a serious and persistent cybersecurity problem. It was not reasonable from an operational or cost perspective to rip and replace the entire network (NASA has an extremely complex network and serves as its own ISP, plus delaying a Shuttle launch was very career limiting). I had to embrace the realization that NASA's IT infrastructure was sorely compromised.

We desperately needed a tactical methodology that would allow us to continue operating while the environment was compromise and/or contested. With this view in mind, in late spring of 2010, I started an effort to identify reasonable and cost-effective technical and procedural solutions that would allow NASA to continue to operate its mission, with high assurance, while the environment was in a perpetual state of compromise.

I reached out to the best cybersecurity Sherpas in the intelligence community requesting assistance and they responded. We had several discussion using out-of-band communications (a key procedure for operating in a compromised environment) and settled on a series of technical solutions that met the reasonable and cost-effective criteria. With solutions in one hand and a tight grip on my lollipop in the other, I was off and running.

In May of 2010, I penned a memo that went out NASA wide that first declared NASA's environment as compromised and second, I provided a series of instructions to regain the trustworthiness of NASA's systems and networks.

Here are the salient excerpts from my 2010 memo:

> "…. A *compromised* environment means that unauthorized individuals or organizations have:
>
> - Successfully accessed NASA's systems and networks;
> - Established the capability to maintain the persistent access to NASA's systems and networks;
> - On demand capabilities to completely control select systems or network infrastructure devices from a remote location (which often times maybe from a country outside the United States);
> - Unfettered access and visibility into various networks, systems, and services (such as email communications) and;
> - Actively exfiltrated NASA's data and information from NASA's systems."

Furthermore:

> "…. A *contested* environment means that unauthorized individuals or organizations are:
>
> - *Using established access to systems and networks with the specific intention of denying, degrading or destroying IT or cyber capabilities, or by altering the usage, product, or the confidence in those capabilities in order to negatively impact our mission."*

Finally, bringing it full circle:

> "The same tools that hostile elements use to threaten and compromise NASA's information systems in order to gain access and exfiltrate data, can be used to degrade, disrupt, or destroy NASA's mission. The key differentiator that is required to migrate NASA's environment from "compromised" to "contested" rest solely on the **intentions** of the individual or organization that has control over or access to NASA's IT system(s) or network device(s)."

Brass tacks and getting down to business

So obviously or maybe not so obvious, the information below is not 100 percent my brainchild. As I stated earlier, I co-opted the collective minds of a handful of cybersecurity and information assurance professionals back in the 2010 timeframe who helped establish the guidance I put forward at NASA. This guidance, as currently written, was regenerated from my notes, memory, and experiences. Most of it will appear as "duh", but one should ask themselves "did I simply rebuild the compute infrastructure, or did I build a known trustworthy infrastructure?"

Nothing in this guidance supersedes or replaces the need to plan for business disruptions of any type. This guidance will not supplant sound incident response practices and procedures. It is not a replacement for business continuity planning or practicing enterprise risk management. It is not a panacea in lieu of integrating system security into the engineering process and designing systems to be resilient. In fact, quite the opposite is true; if an organization does all of the aforementioned functions, then this guidance will most likely not have any relevancy to any user or organization.

And remember, this is not strategic guidance. It is tactical by design. The purpose is to reestablish incremental trust in the compute environment, while said environment is compromised. It should be deployed in byte (yes "byte" because I'm clever) sized increments, building small, highly secure enclaves across the infrastructure and reconnecting those enclaves until trust is fully reestablished with a high level of confidence.

Ok, this is where things get interesting

Whenever the situation arises that requires operating on a compromised network, an action plan should be developed at appropriate levels within each organization. The plan should identify and prioritize actions to be taken by the organization(s) to reduce the risk of operating on the compromised network, identify and prioritize use of the guidance herein, identify who is responsible for each action, identify plans for overall reestablishment of trust on the network, and so forth. This plan would help to tailor the guidance herein to different network environments as well as to different types of compromises.

1. These practices and procedures are to provide guidance for a scenario in which a compromised network needs be used for some limited time until trust can be completely re-established. The guidance provided ranges from reinforcing what should be good cybersecurity hygiene practices to actions that are focused specifically on reducing the risk of using a compromised network.

2. Understand that attacks will vary in severity; thus actions taken should be related to the *perceived threat*. The guidance below has been constructed to be more generic, without considering the severity of the attack or the perceived threat. Some of the actions listed below will improve overall security with little to no cost and should already be the default; others may have major impact on operational usage. Counteraction involves balancing between doing too little and doing too much. Over-reacting to an incident could reduce your organizations capabilities or increase delay; under-reacting could expose business operations to compromise or misdirection by an adversary.

3. The goal is to be able to use the compromised network for business purposes to the greatest extent possible for some period of time, while limiting the information the adversary can extract and the damage an adversary can inflict.

Assumptions

4. A best effort has been undertaken to detect, prevent and clean any known indicators of compromise (IoC) from the network. However, the network is still assumed to be compromised because of what is not known. Confidentiality, integrity, availability, or non-repudiation compromises are all assumed to be possible.

5. There are activities underway to rebuild and re-establish the necessary trust in the compromised network (e.g. re-imaging/replacement of computing platforms and network fabric, cloud environments etc) while it is being used.

6. There will be some reduction in functionality available to network users and using the network may be more inconvenient (e.g. use of specific types of removable media may be restricted, certain protocols may not be allowed, and some applications may not be available).

Generally speaking

7. The recommendations presented here are not intended to be applied universally. Some may not be able to be followed because they would make the network unusable in some instances. Testing of these guidelines in properly designated, high-fidelity operationally relevant testing environments first will be necessary to make sure they do not render the network unusable for business purposes and to make sure they provide effective countermeasures.

8. This guidance should be considered in addition to existing policy and guidance (such as that provided by the Cybersecurity Infrastructure & Security Agency (CISA)). Where there is overlap or conflict, the most restrictive approach should be followed that allows the business to remain operational while minimizing the damage an adversary can inflict on the compromised network.

Operating in a Compromised Environment

Reestablishing trust in critical networking components

There are some critical network assets that must be trusted even on a compromised network. Such assets should be replaced or repaired as soon as possible, even if they are not suspected of having been compromised. Take note that the areas and activities suggested here for re-establishing trust are not all inclusive of what needs to be done to completely clean up the compromised network. They help to re-establish trust to allow the network to be used while still in a compromised state. Activities needed to completely clean up the network are beyond the scope of this guidance.

The most important thing that must be done is to re-establish/regain positive control of network management and administration. Platforms used by system administrators for performing administrative functions must be replaced or repaired.

Other assets that must be considered for early replacement or repair are:

- Platforms performing important network and security management activities such as domain controllers and workstations used for PKI administration.
- Workstations used by critical users such as senior business leaders who are more likely to be targeted than an average user.
- Platforms providing business critical services- A server providing some business-critical service include strategic communications, active directory, e-mail, etc.
- Critical network infrastructure components (e.g. certain routers, switches, firewalls, guards, content filtering, WAFs)

Replacing or repairing a typical computing platform should include:

- 'Reflashing' the BIOS with a known good configuration. Configuring BIOS security/password where available.
- Re-imaging the hard drive with operating system and approved applications (i.e. data center resources). Do not use backups. Platform re-imaging must be done off-line (i.e. in a separate test environ and not on the operational network) to reduce the risk of re-infection.
- Setting proper configurations and locking down the platform in accordance with policy, previously issued guidance, and the guidance listed above. Consider using approved desktop configurations when appropriate.

Tactical procedures

1. Dedicate an Incident Response Team (IRT) that is responsible for proactively monitoring, implementing, enforcing, and otherwise working security for the compromised network. Additional staffing of help desks will also be necessary to address increased user requests and problems.

2. Minimize use of the compromised network to the greatest extent possible. Consider using out-of-band communications for most critical communications instead of e-mail or other communications services from the compromised network. Lockdown and audit VOIP conference call connections (for critical calls related to mitigation efforts).

3. Consider creating a Virtual Private Network (VPN) on top of the compromised network for use by the most critical users or business functions. As the workstations of critical users are repaired, they could be added to this VPN until such time as the entire network has been repaired.

4. Revalidate all user and administrative accounts. This includes those on routers and other network components where login is possible. It also includes revalidating need for remote login accounts. Disable all accounts that cannot be validated.

5. Immediately inform users of the severity of the threat, and the restrictions under which they are operating. Clearly identify actions they will be required to take to help reduce risk to business operations. Keep instructions straightforward. When possible, educate them on the extent of the network compromise so they understand the reason for the added security measures.

6. Force a password change across the networks. This includes all computer accounts, databases, remote logons to network components, etc. Consider a more frequent password change policy. Password changes on accounts, such as database accounts that are accessed via applications, must be coordinated with application owners to avoid users of the application being locked out.

7. Consider backups made between the time of the compromise and its discovery must be as suspect and as high risk and identified with enough information that administrators can recognize the reason for special handling. If data from them is needed it should be restored using an isolated/standalone network and evaluated and cleaned. These backups must not be destroyed. A new, full set of backups should be performed and marked accordingly for replaced, cleaned, or repaired machines.

8. Implement integrity monitoring to detect changes in critical files that should not normally change. When possible, use tools that create a trusted baseline of

cryptographic hashes that are compared to periodic file snapshots to find/detect changes. The process should also list new files and files which have been deleted.

9. Use secure, authenticated login for remote access to servers, desktops, network devices and other network equipment instead of plain text telnet/ftp. For devices that cannot support secure login, implement strict IP address restrictions to permit remote access only from a small set of secure local servers.

10. Ensure that all wireless capabilities are disabled on laptops, routers, etc, or that their need is validated and that they are properly secured. When possible, disable in BIOS or in the operating system instead of in an application. Monitor wireless services for unauthorized local wireless access activities.

11. Ensure that all cross-domain activities that move data between different networks are identified and appropriately authorized. This should include automated Cross Domain Solutions (CDS) and manual cross domain processes. Tighten policies governing cross domain traffic. Furthermore, cross domain traffic should be reduced or more tightly controlled between the compromised network and others. Consideration should be given to shutting off cross domain transfers if they are suspected of advancing the spread of any network malware. If automated filters currently allow encrypted traffic, then perhaps it should be disallowed or allowed only when it can be explicitly identified as valid or inspected (in the case of SSL/TLS traffic).

12. Restrict use of removable media or enforce use in accordance with prescribed directions. Ensure that any media used is purchased or acquired only from authorized sources. When possible, use domain group policy to control use of removable media. Consider treating 'thumbdrives' and similar removable media as accountable property and registered to a specific owner for a specific purpose. Scan and clean these devices on a "trusted scanner system" that implements multiple anti-virus (AV) software after each use.

13. Use encrypted file storage based on individual user keys (e.g. PKI) where possible to limit future loss of data. Move all user data storage from local storage (e.g. C drive) to secure network storage (this may include cloud-based storage) to minimize storage locations and to ease re-imaging/replacement of infected machines. Ensure all such user data is scanned and cleaned. Treat user data that was stored prior to compromise as potentially suspect (see item 7.)

14. Increase monitoring on the network. For example, monitor for network traffic trying to get to the Internet from other domains and monitor traffic to/from cross domain guards.

15. Further limit the protocols that are permitted to traverse enclave boundary firewalls and/or internal segment boundaries.

16. Follow organizational procedures for dealing with any newly infected machines found on the network. If no procedures exist, disconnect the machine from the network and leave powered up to preserve memory contents for forensics analysis.

17. Ensure that anti-malware software capable of detecting, preventing, and cleaning known malicious code from network platforms is deployed to all platforms and is kept up to date. Require that complete scans be regularly scheduled and successfully completed, and that certain activities such as changes to critical registry keys are enforced rather than monitored. If possible, consider using multiple vendors' products as necessary to increase chances of detecting or preventing new infections. Leverage cloud-based endpoint protection services in addition to deployed, host-based anti-malware capability to routinely scan network computers.

18. Encrypt and sign e-mail when possible. Enforce this policy. Make it a default setting.

19. Apply and use all applicable security configuration guidance from CISA, NIST, CIS etc., and secure configs from Microsoft for servers and client machines to the greatest extent possible. This includes locking down browser security settings to most restrictive functionality, disabling all Java Script, Active X controls and similar capabilities in all applications. Allow such scripts by exception only where it is known that a business-critical function may not be performed without them. Assess user complaints for need to readjust exceptions. Use automated mechanisms (e.g. Microsoft Group Policy) to control configurations where possible.

20. Verify and maintain the configuration of all software used on the network at the current acceptable 'patch/revision' level. Validate the authenticity of all 3rd party software updates.

21. Enforce the principle of least privilege for users and machines to the greatest extent possible (e.g. turn off most services, only turning them on if something for that particular box breaks, remove unnecessary/unauthorized programs, disable unneeded interfaces in BIOS, etc.). Use group policy where possible to enforce this.

22. Use a whitelisting of applications that are authorized to run on platforms

23. Restrict client machines from communicating with other client machines, printers, etc. to minimize spread of infection. No Peer-Peer communications for client machines should be allowed. Client machines only communicate with servers and gateways. Leverage the use of Private Virtual LAN (PVLAN) capabilities where available and restrict incoming IP addresses to each client machine when possible.

24. Consider segmenting the network to help isolate critical servers or other platforms. For example, business critical servers could perhaps be firewalled off and controlled to limit access to them. System administration workstations could be isolated in a similar way.

25. Where already available in existing network fabric, use Network Access/Admission Control capabilities to enforce configuration level of computer platforms and to detect and prevent connection of unauthorized network devices.

26. In Windows network environments, closely re- examine all trust relationships for the various Windows domains, particularly those in a "transitive trust" relationship, to ensure they are as expected.

27. Require users to power cycle their computers at least weekly and require that they select 'Restart' when they logoff rather than 'Logoff to reduce the persistence of memory-based attacks.

28. Identify security critical registry keys/settings and set Microsoft Group Policy to audit changes to them. The policy would cause entries in the security event log which could then be reviewed regularly to determine anomalous behavior. Considering limiting this function to the most critical machines on the network (e.g. servers, critical users).

29. Do not allow any electronic devices to be attached to a computer. No personal cell phones, Androids, iPhones, mass storage devices etc. Do not allow the use of any unauthorized removable media.

30. Force enable message receipting capability to help detect potential attacks that affect availability.

About the author

Jerry L. Davis is the founder of Gryphon X, LLC, a full spectrum risk management consulting firm. Jerry has almost three decades of experience in all the classical security domains, including cyber, physical, and personnel security. Jerry is a combat decorated US Marine and a trained counterintelligence officer. Jerry served worldwide with the Central Intelligence Agency (CIA) and as a member of the Senior Executive Service with technology assignments within the United States Department of Education, NASA, and US Department of Veterans Affairs. Jerry is a member of the National Association of Corporate Directors and a Federal Advisory Board member with Smartsheet Inc. Jerry also serves as an advisory board member with Embry-Riddle Aeronautical University, College of Security and Intelligence and is a Fellow with the Institute for Critical Infrastructure Technology, a Washington, DC area Think Tank.

About Gryphon X, LLC

Gryphon X, LLC is a full spectrum risk management consulting firm, focused on technology and corporate risk. Gryphon X supports client engagements across a wide range of industry verticals and is a preferred provider of consultation services such as investigations, executive education, corporate board support, information technology management, expert witness testimony, insider threat program development, 3rd party risk and supply chain risk management among and many others. Gryphon X is proud to be a Mantle Advisors, LLC strategic partner. Together with Mantle Advisors, Gryphon X can provide exceptionally unique risk management and advisory support to a wide variety of organizational needs that are only limited by the imagination.

If you have a need that requires immediate attention or would like more information, contact Jerry.

Email: jldavis@gryphonx.net
Cell: 408.477.7880