HORNECYBER

THE PRACTICAL GUIDE TO SECURITY AT CONFERENCES

WESLEY MCGREW PH.D., DIRECTOR OF CYBER OPERATIONS

CONFERENCES ARE TARGET-RICH ENVIRONMENTS FOR PRIVATE AND NATION-STATE INTELLIGENCE GATHERING.

At the time of publishing, we are in the summer conference season in the information security industry, leading up to the two highest-profile conferences, Black Hat USA and DEF CON. Every year, concerns are raised about the security of operating laptops, phones, and other devices at these conferences. The conferences themselves have a focus on the disclosure of vulnerabilities in systems and protocols, so there is a larger concentration of individuals with the knowledge and means to compromise and monitor such devices.

Ultimately, even if other measures are discussed, traditional wisdom from industry experts is to "unplug." The obvious security benefits of simply not having communications will be presented - usually accompanied by the advice that you'll get more out of a conference without the distraction.

This isn't very realistic, however, for those of us that have a responsibility to be in touch. While a reduction in availability is expected, letting email pile up for four business days is simply not an option for many. Being unable to respond to a crisis, or to assist those who are, may be out of the question. For some, the livelihood of others rely upon their responsiveness.

There's good news and bad news for those who must maintain operational security (OPSEC) and communication security (COMSEC) at a conference. First, the good news:

- Hackers' ability to hack "anything, anywhere" is largely overstated. Knowledge and malicious use of "zero-day" vulnerabilities at conferences against attendees is not as common as is frequently stated.
- It is possible to easily and dramatically raise the bar for the capabilities and funding that an attacker would need to compromise you.
  - By understanding your exposure, deciding what your realistic threats look like, and preparing for secure work before leaving, you can make things much more difficult for an attacker.
- If you are using patched systems and secure protocols, knowledge of a publically-unknown vulnerability might be required to compromise you.
  - To exploit a vulnerability of this nature, in public, is often tantamount to giving it away to anyone else that is monitoring the network.
  - The value of this vulnerability knowledge, and cost of losing exclusivity, may be more than your value to the attacker.

…and now the bad news:

- Conferences are target-rich environments for private and nation-state intelligence gathering.
- Outside of the context of an organized conference, the same threats exist at hotels, coffee shops, and other places that are frequented by "road warrior" workers.
- Devices often "leak" identifying information in their default configuration.
- Common practices in mobile work/communication are not sufficient in repelling a targeted attack, even if the target is as broad as "attendees of the same conference."

The threats and mitigations in this guide were written with a conference like Black Hat USA or DEF CON in mind, where the presence of an attacker with the full capability to use publicly-known vulnerabilities can be assured. The same measures are, however, applicable to any conference or work-travel situation. It would be a mistake to assume that the same attacks wouldn't be launched against you in another environment. If anything, an attacker might find easier and more valuable targets at a conference of non-IT industry professionals.

The exact software and techniques you use to implement these recommendations will vary based on your exact needs, the work you do, and the network environment you need to "phone home" to. For that reason, I avoid descriptions of specific software. If you find the implementation of these measures difficult without specific instruction or recommendation, you need the services of an information security professional to assist in setting yourself up to secure your mobile work. The devil is truly in the details of getting this right, but if you are an information security professional, none of this should provide a challenge.

This approach also has the benefit of making this document a little more timeless than it would be otherwise. The only concession is a discussion of contemporary network technologies and descriptions of the state of the art in threat actor capabilities. These will evolve, though for now I would argue that this advice has been relevant for a number of years.

I hope that you find this guidance valuable. I believe, assuming a relatively small degree of risk, and addressing the rest sensibly, it is possible to communicate and conduct some amount of business from within a "hostile" network environment. Conferences such as Black Hat USA and DEF CON have a reputation as being the most hostile in this sense, however, I believe they are fundamentally no more dangerous than any conference, or even any more than your average hotel network.

ATTACK SURFACE

Attack surface can be defined as the set of interfaces and interactions an attacker can have to a target. A vulnerability in a part of the attack surface can lead to access to a device, or disclosure of communications.

To maintain the security of your devices and communications while traveling, the overall theme should be that of reducing your attack surface. Most of the advice in this paper involves reducing attack surface.

For example, a laptop, without a software-based firewall, likely has a large attack surface. Obvious elements of the attack surface include listening network services, such as file sharing, development web servers, and portions of your endpoint protection system (something we've noticed on recent engagements). Less obvious elements include the desktop software you use. Every web server you connect to gets to throw arbitrary input at your browser.

Protocols also represent attack surface. Windows and other desktop operating systems frequently announce their presence on a network, and seek out other local systems to communicate with. The protocols used to browse the web, chat, or check email is subject to interception or modification in transit. Strong and well-implemented encryption is required to prevent a compromise of confidentiality.

While all of these elements can be addressed individually, with specific hardening techniques, the most secure answer is the easiest: turn it off. This is easier said than done, if you have an operational need for the software or service.

THREAT ACTORS

While an information security conference may have a higher concentration of these threat actors present, there is no reason to assume their absence from conferences in other industries. Any place that provides service for workers on the road – including hotels, coffee shops, and airports – will be attractive for attackers as well. Here are some very basic profiles of the threat actors that you might seek to take advantage of poor OPSEC/COMSEC while you're working outside of the office.

- **Thieves** – Primarily interested in the intrinsic value of your devices, it may also occur to some that it would be worth checking for valuable data before wiping the device and attempting to sell it.
- **Unsophisticated Attackers** – The vast majority of "hackers" at conferences will fall somewhere in this category. They are largely opportunistic, and may not have well-defined motives other than opportunistic embarrassment or profit from victims. These attackers will be armed only with publically-available exploits and tools, giving them the capability to attack unpatched systems and monitor or intercept encrypted communications. Good computer "hygiene" with regards to patching and use of protocols where endpoints can be verified with certificates (such as most VPNs) will prevent these attackers from having much success. These attackers may be:

    Passive – In that they only monitor wired and wireless communications without directly interacting with endpoints.

Active – Actively using fake access points and "man-in-the-middle" attacks, such as those provided by off-the-shelf devices like the Wi-Fi Pineapple.

- ***Moderately-Sophisticated Attackers*** – While still opportunistic and untargeted, attackers in this category have capabilities that are difficult for unsophisticated attackers to acquire from public security knowledge or off-the-shelf tools. They may have the capability to deploy fake cellular base stations in order to attempt to intercept mobile device communications, though it is our experience that they're more likely to accidentally disrupt cellular networking than successfully intercept it.

- ***Organized Cyber Criminals*** – In this category, you have attackers that are motivated by profit, with capabilities that are backed by funding. Such attackers may target specific companies or individuals. They are much fewer in number than opportunistic attackers, but may have the capability to launch attacks using "zero-day" exploits or techniques that are not publicly known.

- ***Intelligence*** – With corporate or nation-state espionage as a motivation, an attacker is likely to be selective with targets and well-funded out of proportion with other threat actors. In this category, there would be much less aversion to attempting physical compromise or in-person social engineering. Interception ability is defined closer to the theoretic limits than by what is publicly available. While much, much fewer in number than the others, it would be a mistake to assume that they are not present. Ultimately, the measures you take can make it much more difficult for these attackers, but if you are the specific target, you can only hope to limit the compromise as much as possible.

When considering the threat actors that might be in your vicinity, it's important that you shouldn't "seize up" and simply not communicate or work at all (unless that is a luxury you can afford). A balance can often be struck by implementing secure practices that exclude lower-capability attackers (the vast majority) and limit the damage that the very few sophisticated attackers can cause by restricting the things you access and expose to the bare necessities.

PHYSICAL SECURITY

Security starts with physical control over your devices. Your mobile phone is the easiest, as you're likely to have that on you at all times. For your laptops and other devices, having them in your bag during the day might be practical and safe, but you're unlikely to want to bring them along for dinner and drinks in the evening and night. A hotel room safe is perhaps better than leaving the devices out on the bed, but is not completely trustworthy. By no means should you leave your devices unattended outside of your room, such as in a conference's briefing hall during a break.

You are far more likely to experience common theft of your devices by those hoping to get some value in selling the device itself, than any sort of advanced tampering that would be associated with espionage. Whole-disk encryption, provided by most modern operating systems, is effective in preventing opportunistic or targeted analysis of stolen devices. An encrypted drive is strongest, however, with the device in a completely powered-down state, reducing the likelihood that an encryption key could be recovered from volatile memory.

If you are concerned about hardware being modified (for example, to log your keystrokes, capturing your encryption passwords and more), then you have a much more difficult road ahead of you. Either get used to being inseparable from your backpack, or move forward with the assumption that the hardware will be compromised. Limit your exposure by conducting business through the only device you are always carrying with you – your mobile phone – or limit your exposure by changing passwords after the conference and restricting your own access to data while there. If tampering is a concern, you will have to treat the device as compromised on return, and disposal is the only option that will ease your mind – I hope it was cheap! This is above the level at which you'd expect an opportunistic attacker to operate. It would take targeting by a highly motivated attacker to assume the risks associated with covert entry and modification of your hardware.

This may sound very frightening, but your most common threats are not going to go to this length. Whole-disk encryption and common-sense theft prevention are going to prevent most attackers from posing a physical-access threat. Modification of hardware to assist in monitoring or subverting encryption is beyond the off-the-shelf capabilities of most attackers, even including the overwhelming majority of security conference attendees.

If you are traveling internationally, your risks go up considerably. You are not a citizen of the country you are traveling to, and may represent a legal and/or attractive target to law enforcement and intelligence. In these cases, "disposable" hardware is a must. You are also subject to search at borders, and may be compelled to provide passwords for encryption. At those times, have nothing sensitive on your laptop. Access that information over the Internet using a VPN or other encrypted protocol at your destination, and make sure it's securely wiped from your device before you make your return trip.

PASSWORD SECURITY

For all accounts that you intend to access "on the road," a change of password before leaving, and a change upon your return is prudent. Passwords should be complex: at least 12 characters, upper and lower case, numbers and symbols. Passwords should not be re-used between services.

The change before the event is primarily to prevent a disclosure from providing access to other services and encrypted files for which the password will not change before, during, or after. If you're already following the secure practice of not re-using your passwords, then this is less of a concern. The change post-event is more necessary.

Passwords may be inadvertently disclosed during the event for several reasons, including:

- ***Shoulder-surfing*** – In crowded environments, it may be difficult to discreetly enter your passwords while controlling line-of-sight to your keyboard or touch-screen.
- ***Phishing*** – The distractions of the event can contribute to less vigilance with identifying phishing attempts, especially those targeted at attendees. The disruption to your routine, logging into systems in a different manner than you did at the office, can cause you to be less likely to identify phishing attempts.
- ***Compromise*** – Despite your best efforts and practices employed from this guide, your devices or communications may be compromised. By changing passwords, you may be able to limit the duration of a compromise.

Changing passwords, however, also presents a problem. Locking down everything with new passwords asks for a situation where you have forgotten those passwords and are now dead in the water for accessing the services you need. You now have the problem of securely coordinating a password reset with someone back at the office. It's unrealistic for most to memorize all of the passwords needed, without some assistance.

To avoid this problem, employ two measures:

- Make use of passphrases instead of passwords. Random sequences of four or more dictionary words, with intentional typos and replaced/interspersed characters, can be easier to remember than a random sequence of twelve characters.
- Password management software can be used to store passwords in an encrypted form. If you can remember your master password to access the manager, then you can access your others. Password management apps are available for smartphones that allow you to access your passwords from the device you intend to always have in physical possession.

Memorable and strong passphrases can be used for your password manager, whole-disk encryption passwords, and other frequently used or critical services. The remainder of your passwords can be randomly generated and stored in the password manager. Avoid cloud-based management of passwords, if connectivity to that service may be difficult to maintain.

Saved/pre-filled passwords are usually a trade of security for convenience. In practice, however, the benefits may outweigh the risks. A pre-filled password does not have to be typed in the presence of others' prying eyes. Having a stored password also gives you the luxury of making it very complex, without having to memorize or type it accurately. Saved passwords may be at risk if your device falls into the wrong hands, though device encryption may help mitigate this – at least until you are able to change passwords. You will not be able to have your device encryption passwords pre-filled (and rightfully so).

Two-factor authentication improves matters considerably. A compromised password is less useful to an attacker if a physical token is also required to use it. Two-factor mechanisms that utilize SMS messaging or email are less secure, and subject to the reliability of your cellular or Wi-Fi connection. Two-factor authentication should be implemented where it is feasible, while being mindful about keeping physical control over the token.

DEVICES

Measures taken to prevent physical access and theft can only go so far. The next layer of defense is to encrypt the information on devices (such as laptops or mobile phones) in order to prevent the exposure of data in the event of theft or other physical compromise. Modern operating systems for laptops and mobile devices support encrypting the device's storage, requiring a password to unlock the device at startup or when waking from a sleep state.

The key to effectively using device encryption, however, is to understand what states of the device are protected by encryption. When you are logged into a device, the encryption key is in memory and being actively used to access that encrypted disk. If you leave a device unattended while it is logged in and unlocked, the encryption will do you no good. If you leave the system on, but log off or lock the screen, you have made it more difficult to recover the key from memory if the device is physically compromised.

The safest state for an encrypted device to be in is for it to be powered off when not in use. By reducing the chance that an encryption key can be recovered from memory, you are making the data much more difficult to access. When device encryption is used correctly, you have raised the bar for attackers up to the point that it would only be readable by an advanced adversary with the capability to surreptitiously modify your hardware to capture your password, or less likely the capability of cracking the encryption.

Device encryption does not protect your system from network-based attacks. There are, however, common sense best practices for reducing your attack surface and harden laptops and mobile devices.

Laptop Computers

A clean installation of your operating system, with the minimum set of software needed to conduct your work, should serve as a good starting point. A host-based firewall solution, configured to restrict everything, allowing only very specific traffic necessary for your work, will help to reduce your attack surface as well. Test your system by using it to connect to the systems and services you will need to ensure you have everything you need once you're out of the office.

Before departing, update the operating system and all software installed to the latest available versions. Once you have done this, it may be prudent to disable automatic updates for the duration of the trip, as some software update mechanisms can be leveraged by attackers to compromise a system. If necessary, check for updates manually after establishing a secure VPN connection back to your office.

Privacy screens are available for laptops that reduce the effective viewing angle of the screen. This can help reduce onlookers' visibility of your screen while using the device. This is not foolproof protection, however. Even with a privacy screen, you should still be aware of your surroundings, as someone directly behind you could still read the screen.

Configure your screensaver to engage on a very short delay, and require a password to unlock the screen once it does engage. Learn the keystroke combination required to quickly lock your screen, and make it a habit to do so whenever your attention is drawn away from your computer. When you are not making active use of the laptop, power it down completely to leave it in a safe state.

Mobile Devices

A mobile device, such as a smartphone or tablet, can provide a much safer computing environment than a laptop. While general-purpose operating systems are designed to run arbitrary code from any source, providing a friendly environment for malicious software, mobile operating systems are designed at a fundamental level to prevent the execution of unsigned and unverified code. Jailbreak hacks, debug, developer mode, and other similar configurations and modifications disable many exploit mitigations and should be avoided on a mobile device, if you wish to make exploitation and post-exploitation activity difficult for an attacker.

A clean restoration of the device to factory settings, minimizing the number of apps required to perform your work, is an excellent starting point. Update the OS and apps to the latest available versions before departing, and turn off any automatic updating for the duration of your trip. If a critical security update is verified publicly as being released during your trip, it may be difficult to establish whether your copy of the update locally is coming from a secure source or not. In the event that this occurs, it may be safer to discontinue usage of the device.

A "burner" phone may be tempting to implement, though the benefits of the anonymity of such a device might be lost if you have your work calls, texts, and other communications forwarded to it. Such a device may help you communicate with other team members at the conference, but will be of limited utility in getting real work done. Unless your burner is stripped of most smartphone features, it is not likely any safer from being compromised than your daily-carry phone. In the end, it will be another device to carry, likely not replacing your smartphone, and you will have to decide if it fits your use case.

When charging your phone, only do so from your own wall adapter, laptop, or battery. USB ports and charging stations in hotel rooms, conference areas, and other public spaces can be configured to extract data from or otherwise interact with your phone in malicious ways.

Other

Smart watches, fitness trackers, wireless headsets, and other devices that connect with Bluetooth and other low-power networking are not likely necessary for your work. The Bluetooth protocol frequently leaks information about the presence of such devices and their owners. It's simply an unnecessary part of your attack surface and it's recommended that Bluetooth devices should be left at home, and Bluetooth receivers should be disabled on mobile devices and laptops.

NETWORKING

Virtual Private Networks

The first order of business in communicating and working securely in the field should be to use the local network to gain secure access to a more trusted network. Wi-Fi provided at a venue, or the cellular network, may be your medium for accessing the Internet, but you can reduce the amount of trust you must place in it by using a Virtual Private Network (VPN) to connect back to the office or other secure location. The specific VPN technology you use isn't as important, as long as it supports strong encryption and authentication (of both the client and server), and is supported by your laptop and smartphone.

The VPN should be configured to route all network traffic on the connected device through the encrypted tunnel, and you should become familiar with what public IP address or range you will have when connected to that VPN. If you perform a Google search for IP address, it will tell you your public IP address. You can use this to help verify that your connection is being correctly routed before conducting any other activity. On the server side, the network subnet in which remote VPN users are allocated should be configured to only allow access to the services that are needed for the remote workers, and if possible, should be monitored during the conference for unusual behavior.

A problem with a VPN connection is controlling "chatty" applications on the network when the VPN is not connected. Many operating systems happily announce their computer names on the local network, and applications that run in the background and/or on startup will attempt to make connections for software updates and notifications. This may leak more information than you desire, or open up some of your software as attack surface while not associated with the VPN.

Configure software (such as your email client) to not start immediately on boot or login, and start that software manually once you have verified that your VPN is connected. If possible, configure your servers such that the client software is not allowed to connect unless it is coming from a trusted IP address range. Your email client and other necessary

programs should be configured to use encryption when connecting to their servers, as well. The VPN simply acts as another layer of protection, reducing the amount of metadata available to eavesdroppers, and acting as a safety net for unencrypted protocols such as plaintext HTTP web browsing.

Leveraging Virtualization

This scenario provides a good use case for virtualization. A minimal host operating system with the ability to connect to your VPN would allow you to start up and verify that you have a secure connection before turning on a virtual operating system environment that contains the tools and configuration needed for your communications and work. Another benefit of this configuration is that a "snapshot" can be used to revert the virtual environment back to a "known good" state after each use. Malware and compromises based in software vulnerabilities will have a harder time persisting in this environment.

Mobile

Mobile phones and tablets are also able to connect to VPN servers. Your options may, however, be more limited in what server software can be used. Mobile applications are also designed to continuously make connections in the background, making it difficult to restrict the amount of non-VPN traffic you generate. You should disable accounts when possible, only re-enabling them when you are making a conscious effort to use them after verifying connectivity to your VPN server. Where possible, restrict applications' ability to transfer data while in the "background."

Wi-Fi vs. Cellular

This can be a more difficult choice than you would initially suspect. The bar for entry on monitoring and manipulating Wi-Fi traffic is much lower, allowing more attackers to interfere with your communications. The vast majority of those attackers are, however, not very sophisticated. If you are well-versed in Wi-Fi yourself, it will be very easy for you to identify most Wi-Fi attacks. A rogue network or man-in-the-middle attack may pose a risk for unencrypted communications, but you are likely building the assumption that this "hop" is being monitored into your practices anyway.

While a WPA2 Wi-Fi network with unique usernames and passwords, such as the one DEF CON runs for attendees, may be more resistant to attack than the unencrypted networks found in most venues, it does not mean that it should be considered a trusted network. You do not control the wired network it routes to, nor do you have any control over its infrastructure. It is still simply a means for you to establish your own secure communications.

Cellular networks have a higher price of entry for attackers in both cost and knowledge required to successfully intercept or manipulate. Fake base stations and forced downgrading of supported services will likely be part of the attack. If your phone is susceptible to these attacks, it might be difficult to protect voice and SMS communications. Much like on a rogue Wi-Fi network, however, a breakdown at this "hop" in confidentiality does not necessarily impact your ability to connect to your VPN.

Your phone and its cellular "baseband" radio are much more of an opaque black box to you as well. It will likely be difficult to tell if you are being targeted or if an attack is ongoing. If you are a savvy user, it is more likely that you will identify malicious operations using Wi-Fi than more advanced attacks targeting your cellular communications.

The takeaway here is that for IP-based communications, it really shouldn't matter since your threat model should take it into account either way. One may be more reliable, with regards to service level and speed, than the other at your location. You may wish to avoid the use of voice calls and SMS or limit the nature of the conversations carried out over those media.

Ultimately, whether you choose to connect through Wi-Fi or the cellular network, it should be treated as an untrusted network. It should only be your first step in establishing a more secure channel to communicate. When the network you chose does not allow you to make that secure connection, do not let it force you to degrade your practices in order to communicate. Choose another or do without. An attacker that is frustrated by your use of a VPN might block that traffic in the hopes that you will revert to more insecure practices.

Wired Networks

Many hotel rooms still provide wired Ethernet access to the Internet. While communications over the Ethernet network are not subject to over-the-air interception (unless it is being bridged with the wireless network), one should not assume their communications are any more private or secure than they were over the wireless. There are many effective means for man-in-the-middle attacks on local wired network segments, and the network infrastructure may be compromised. Treat it no differently than you would a wireless network – as though anyone could be watching.

SOCIAL MEDIA

Social media is a part of how some people do business. While it's easy for some to exclude this from their "necessities" on the road, it's an important part of staying in touch with colleagues, promoting a personal or company brand, or even to provide an informative service to others. Social networking can take place in the context of the measures discussed earlier, but you may find that to be cumbersome – hurting your ability to dynamically check, post and receive alerts.

You may wish to compromise by allowing usage of your social networking applications outside the context of the VPN and other measures that you take to protect more sensitive data. This is not entirely unsafe, as most social networks make use of client to server encryption, though you would prefer more layers of

defense against more sensitive data. If this is the route you want to take, it is recommended that you take some basic measures to improve your account's security posture:

- If possible, enable two-factor authentication.
- Check to make sure you have access to the email account associated with the social networking account.
- Change the password before and after the event, and do not reuse passwords across multiple accounts. Specifically, do not reuse the social networking passwords on your own sensitive systems.
- Before the event, delete all private communications from the account.
- Ensure that the account is not being used to authenticate accounts on other, more sensitive, services.
- Review the applications, add-ons, or API access that the account is configured to provide to third parties before and after the event.
- Stick to the cellular networks for social networking, avoiding the majority of attackers who are limited to operating on Wi-Fi.

You may use the same techniques for "throwaway" chat accounts used to communicate with friends and colleagues at the same event.

To prevent more sensitive applications from communicating while you are connected to a network with your social media applications, you may wish to segment your activities, relegating social media to a separate device for the duration of your travel.

SOCIAL ENGINEERING

"Social engineering" is a term invented by information security professionals in order to sound more legitimate than the equally accurate "con artistry." Psychological manipulation predates this field and is not limited to phone calls and email. The in-person elicitation of sensitive information is a common and real threat.

Over drinks and among peers, it is tempting to disclose secrets in the form of "war stories." Avoid that temptation, especially when it comes to clients that have placed trust in you. Innocuous questions may lead to a more accurate profile of your organizations' operations than you would have been comfortable disclosing directly.

FINANCIAL

When you trade the relative (though not complete) anonymity of cash for the convenience of plastic, you have already given up some degree of anonymity and privacy. It only takes a glance at the news to realize that point-of-sale terminals, vendors, and payment processors alike are being targeted successfully. If you are trying to protect information about your whereabouts and purchasing history, then cash should be your go-to.

If your primary concern is the protection of your finances, however, things get simpler. Use credit cards. While a breach, disclosure and theft of your payment information may be inevitable, as a consumer there are legal protections in the US that limit your liability in the event that your card is subject to abuse. A debit card, or other form of payment, may not have the same protections.

Avoid online banking on a hostile network. In the best case, even with encrypted traffic, an attacker can identify what bank you are communicating with and use that information to build an impressive targeted phishing campaign against you. Restrict that activity to a VPN session, if it is necessary. If possible, have a trusted family member back home take care of bills and checking on your finances while your away.

CONCLUSIONS

The most hostile network, however, is not specific to any conference, it's the public Internet we use every day. When you step outside the confines of your private work network, you are subject to attack. While you may not have the option to unplug, with the right mindset you can establish a channel through which you can communicate and work with a level of trust that fits your needs.

The key concepts you should remember and let guide your actions are:

- Minimize your attack surface.
- Establish the bare minimum of software and communication necessary to conduct your work.
- Physically protect your devices.
- Use secure, unique passwords – and manage them well.
- Layer security around your network activity with encrypted protocols, VPNs, firewalls and the implementation of other best practices.
- Do not depend on the security of networks to which you connect.
- Make smart decisions based on the kind of data you need to protect, and the capabilities of your likely adversaries.
- Be aware of the environment in which you're operating.

ABOUT THE AUTHOR

Wesley McGrew, Ph.D.

Wesley serves as the director of cyber operations for HORNE Cyber Solutions. Known for his work in offensive information security and cyber operations, Wesley specializes in penetration testing, network vulnerability analysis, exploit development, reverse engineering of malicious software and network traffic analysis.

HORNE CYBER