

THE OPEN SOURCE



CYBERSECURITY PLAYBOOK

WRITTEN BY PETE HERZOG

CONTRIBUTORS



Contents

03 Part 1: Scouting Reports

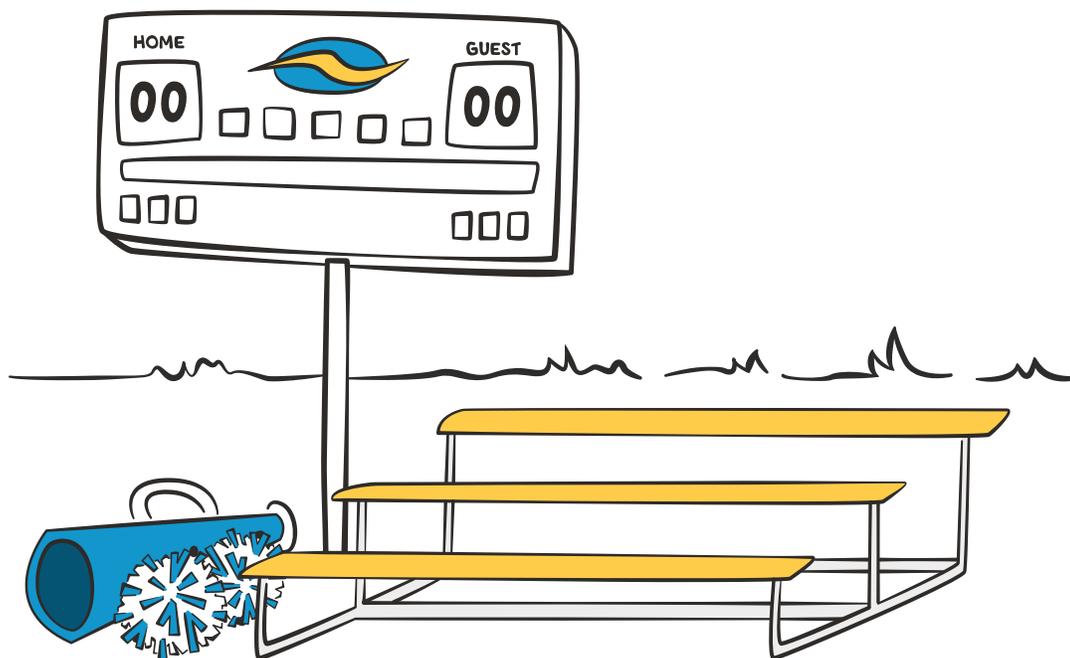
Profiles for ten of the most common threats you should be prepared to face.

10 Part 2: The Game Plan

A practical, step-by-step process for making your organization more secure.

19 Part 3: Looking Downfield

Set yourself up for success both now and in the long run as threats evolve.



Part 1: Scouting Reports

What security threats should I be prepared for?

The first key to any effective security game plan is knowing what you're up against. In this section, you'll learn all about ten of the most common threats your company is likely to face.

While by no means comprehensive, this list can help you better understand some of the tactics being directed against you and your users, along with the specific reasons you're potentially vulnerable to each.

From phishing to ransomware to distributed denial of service (DDoS) attacks, the more you know about these threats the better. They're some of the leading causes of data breaches, downtime, and a serious lack of sleep.

→ Phishing

What it is:

Any attempt to compromise a system and/or steal information by tricking a user into responding to a malicious message. The most common phishing attacks involve emails armed with malware hidden in attachments or links to infected websites, although phishing can be conducted via other methods such as voicemail, text messages, and social media, too.

What makes protection a challenge:

For one thing, employees are already in the habit of clicking things because that's how you interact with modern computers. For another, phishing emails are much more sophisticated than they used to be. Scammers can take over legitimate email accounts or spoof their email addresses to make it look like messages are coming from someone employees trust.

Once a victim is tricked and becomes compromised, the attacker now has their access credentials. They can reach all the same servers, log into the same web applications, and download the same files as if they were that employee. The challenge with protecting against this is you need to limit what servers employees can access or how they can access them. There are times that may run counter to what they need to do their jobs.

Additionally, even if you train employees to be on the lookout for suspicious emails, some phishing attacks can be extremely targeted and look just like any other email from a trusted source who is being impersonated. The most convincing examples of these "spear phishing attacks" don't provide any red flags until it's too late.

→ Social Engineering

What it is:

There are two ways to steal anything – you either take it yourself or you get someone else to give it to you. Social engineering is a broad umbrella term for any tactics designed to exploit and manipulate trust, so the victim hands the attacker what they want – access to information, accounts, or computers inside a secured area. Think fake customer service calls designed to reset passwords or a criminal spoofing your CEO's email address and asking someone in finance to send an urgent wire transfer – a type of scam referred to as a **business email compromise (BEC)**.

What makes protection a challenge:

Everyone – repeat, everyone – can be conned, defrauded, fooled, or manipulated. Being vulnerable can sometimes come down to a lack of training or experience, but more often it can simply come down to distraction and mental fatigue.

Since this attack targets people directly there's very little that technical safeguards can do, especially if the action isn't outside the employee's typical responsibilities or usual behavior – like resetting a password for a desperate user (a typical tech support con).

➔ Ransomware

What it is:

Malicious software designed to encrypt a victim's files and then demand payment, generally in anonymous Bitcoin, in exchange for decrypting the files.

As with other malware infections, ransomware attacks typically start with employees falling victim to phishing emails or visiting compromised websites. Unlike other malware infections, however, the primary goal of ransomware isn't to gain stealth and persistence for long periods of time. Instead, its priority is to spread as quickly as possible, encrypt as much data as possible, then actively alert victims of its presence so criminals can extort them.

What makes protection a challenge:

Ransomware will lock up any drive the employee has access to, including connected USB drives and network shares. Once files are encrypted the only way to regain access to them is to a) hope you have a reliable, up-to-date backup; b) hope a security researcher has cracked the encryption and made a decrypting tool available; or c) hold your nose and pay the ransom. Paying up is anything but a sure thing, because, well, ransomware authors are criminals. Being dishonest is what they do. They're also occasionally less than spectacular at coding, so there's also the risk of paying the ransom only to find your files were accidentally destroyed or rendered unrecoverable.

One reason ransomware is hard to protect against is because it's built to turn a strength – making files accessible across an organization – into a weakness. Additionally, with ransomware developing into a billion-dollar industry, there's plenty of incentive for criminals to continue investing in delivery and evasion tactics to keep their business model humming. That means they can change faster than your signature-based security solutions can keep up.

➔ Downloaders

What it is:

Normal-looking programs designed to fetch and install malware without raising any security alarms. In effect, what downloaders allow attackers to do is to get a "man on the inside" prior to committing to a full attack (it's no coincidence they're typically called "trojan programs"). Once a downloader creeps its way onto a victim's system it can scope out the security settings, then smuggle other dangerous malware in after it's established the cost is clear. Even after an attack is discovered and the other malware has been removed, as long as the downloader is still there hiding away, it can grab more malware and start the process all over again.

What makes protection a challenge:

Downloaders are one step removed from the actual dirty work involved in executing an attack. That means they don't have to pack the same kind of functionality that might get other malware blocked. Instead, malware makers can focus solely on designing downloaders to be extremely good at avoiding detection.

Think of it as attackers choosing to have a team made up skilled specialists rather than mediocre generalists. The downloader is a prolific passer and the malware it downloads is a sensational scorer. With both of them able to focus on their respective speciality, they're able to be much more effective when paired together.



Drive-by Downloads / Download Hijacking

What it is:

In nature, the big predators hang out at common water holes and wait for their prey to come by. On the Internet, the big predators find ways to turn popular website visits into covert attacks. In some cases, they inject code through comments that force unsuspecting visitors to automatically download malware. In other cases, they compromise the web server and inject malicious code into seemingly legitimate downloads. Another trick is to utilize exploit kits, programs designed to actively probe the website visitor's system for software vulnerabilities that can be exploited.

What makes protection a challenge:

Not only do attackers have the element of surprise in these situations, they also have a collection of tricks to make sure they're successful. If you update your browser, they'll update their code. If you patch a vulnerability they'll move on to a new one. It's also not as if we're talking about strictly sketchy websites. Some of the web's most popular sites (The New York Times, the BBC, AOL, the MSN homepage) have been compromised in the past. You usually can't ask employees to stop using the Internet altogether.



Malvertising

What it is:

Marketers aren't the only ones who like to utilize advertising to get in front of the crowds of website visitors. Criminals do the same thing, creating fake ads or inserting malicious code into legitimate ads so they can quite literally capture their audience.

What makes protection a challenge:

Online advertising is already incredibly prevalent and chances are it's only going to grow more aggressive. At the same time, people are also becoming increasingly used to ads, including pop-ups, etc. and they're no longer viewed with as much mistrust. In terms of protection, the quick knee-jerk reaction is to use ad-blocker software. Unfortunately, many websites don't work unless you deactivate it. And if employees have to choose between their ad-blocker and a top 10 list of cat videos...

→ Zero-Day Attack

What it is:

Traditionally, a zero-day refers to any undisclosed vulnerability that attackers can exploit before victims and software vendors become aware of it and have the chance to patch it. The term “zero-day attack” is also sometimes more broadly applied to attacks that utilize new tactics, exploits, or malware variants that haven’t been seen before, giving them an advantage.

What makes protection a challenge:

It’s difficult to protect yourself against something you’ve never encountered before, especially if it blindsides you. Signature-based security solutions are particularly susceptible to getting bypassed by zero-day attacks since the way they identify malicious files is by comparing them to a list of previously captured malware samples to see if there’s a match. If an attack is using a never-before-seen exploit or piece of malware, there’s a good chance it’s going to claim a victim.

Because of their effectiveness, zero-days are in high demand, and criminals have become increasingly incentivized to discover more of them. Unfortunately, that means uncovering and patching one vulnerability may only offer you momentary protection before attackers move on to exploiting the next one.

→ Password Cracking

What it is:

A login and password isn’t what most people think it is. It’s actually a complicated set of processes that can involve multiple systems, secure transport to and from the servers, a trusted network of server identity assurance and revocation, code to evaluate the complexity of the user-generated password, more code to make sure the person entering the code is indeed a human, a secondary factor of authentication, and a means to recover lost passwords. So password cracking is more than just running a program to guess the password — it’s about cracking the password process to take over a user’s account.

What makes protection a challenge:

Any system that allows users to access it from anywhere and also requires those users to make, safeguard, and remember their own passwords is a system that’s going to be difficult (if not impossible) to defend.

According to what OSSTMM researchers refer to as “The Somebody Sequence,” the more interaction somebody has in the security process, the greater its attack surface. Asking employees to manage their own passwords is like giving them full control over the keys to an important lock. You can purchase one of the strongest locks money can buy, but how secure can it ultimately be if there are keys for it floating around everywhere?

➔ Distributed Denial of Service Attack (DDoS)

What it is:

There is only so much traffic a computer system can process before it starts to slow down and becomes overwhelmed. By gaining control over a large number of hijacked systems and devices (referred to as a botnet), attackers can direct large amounts of connection requests or packets of random data at a single target all at once, with the intention of overloading the system and taking it offline.

What makes protection a challenge:

The larger the botnet, the more damage a DDoS attack can do. The best you can hope for when you're attacked is that you're subscribed to an anti-DDoS service, but even that doesn't provide a guarantee you'll stay up and running if you're dealing with an attack with a high level of magnitude.

To make matters worse, sometimes attackers will contact their targets ahead of time and threaten to knock them offline unless "protection money" is paid up front. It can be difficult to discern whether such threats or simply scams, and — as is the case with ransomware — giving in to criminal extortion demands never comes with a guarantee.

➔ Scareware

What it is:

You've probably seen the pop-ups — "Warning! A virus has been detected on your computer. Download VirusBlaster to clean and remove it." The malware that really infects your computer is the program that pop-up is trying to trick you into downloading. Scareware can come in a variety of forms from fake antivirus programs to fake browsers or software updates.

What makes protection a challenge:

We know that social engineering works because it preys on the distracted and mentally fatigued. Combine that with eagerness to please or help and thus begins the "good intentions" downward spiral that leads employees to make really bad decisions.

Once scareware gets inside the system it has all the privileges, passwords, and logins of the employee who installed it. Getting it out may be as easy as just wiping the system and starting fresh or recovering from backup. Or it may be more difficult and time-consuming if the malware spreads to other systems.

SQL Injection

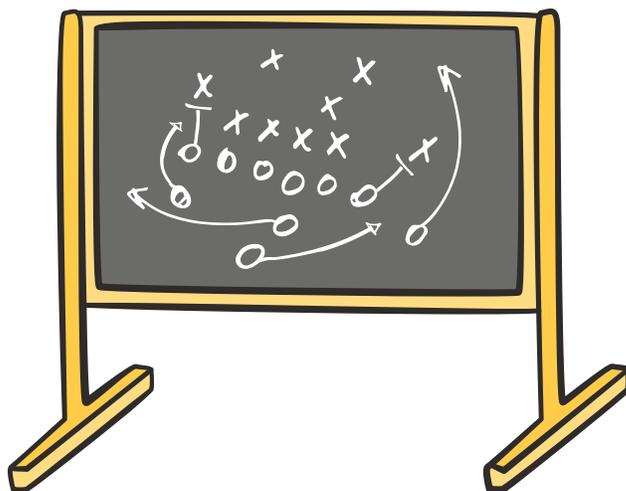
What it is:

If a website has an input box or entry form (like when you're entering in your username and password, or your credit card number if you're buying something) then an attacker can try inserting structured query language code to gain access to or make changes to the stored data.

What makes protection a challenge:

SQL injection exploits a trust between the web application and its database to let the attacker do pretty much whatever it wants with the database. If all you can think of is "delete data" then you're underestimating the depths a criminal can stoop to. Besides adding, removing, and changing data, and in addition to stealing info like client credit card numbers, personal data, and health records, there's also the possibility of inserting malicious code to be passed back to users when they use the form, instead of the data they're looking for. Once criminals start using that tactic they can abuse popular websites to do their dirty work for them like distributing drive-by downloads, building a botnet army, even hijacking DNS requests to send visitors to malicious versions of legitimate websites they know and trust. If the login form is vulnerable, SQL injection can even help with password cracking by the bypassing the login altogether.

Any place where a user can input information into a website with a database, it has the potential to be SQL injectable, which unfortunately makes it a widespread problem. You can't just remove all user-input interactions from your website and still get any purchases or feedback.



Part 2: The Game Plan

As anyone who's ever been on the wrong side of a data breach can attest, security is not a game. First of all, the stakes are real. But also unlike a game, there are no set rules or boundaries. Even if there were, attackers aren't exactly known for their fair play.

That said, we do tend to discuss security using sports terms. There is an offense with attackers and there is defense. The goal of the defenders is to stop the attackers, to prevent them from accessing or causing damage to our assets. This is done through defensive tactics just like the attackers apply offensive tactics.

The biggest problem is we don't always know the parameters of the "game" we're playing with attackers until it's too late. We don't know who our opponents are. We don't know their capabilities or their goals. Is it stealthy, silent robbery or a quick smash and grab for data they can quickly encrypt and ransom? Are we their target of hate or are we a moment of opportunity for them?

As a result, we're pressured to develop tactics that can somehow be equally effective against a diverse and rapidly growing variety of potential attacks. Worse, our defenses also have to take into account the operational needs of the business. Not only do we need to stop attacks, we also need to ensure our security measures don't also slow or stop any processes or services.

An attacker has no such limitations. As such, the first thing any game plan for our security efforts has to take into account is that attackers and defenders aren't playing by the same rules. The playing field is anything but level.

An attacker only has to be effective against one specific aspect of our defense — by any means possible — in order to be successful. As a defender, meanwhile, we have to be effective against all manner of potential attacks. And we have to operate under economical limitations, legal restrictions, and industry regulations.

With the game so stacked against us, what does a winning strategy for defenders look like?

Create a Zone Defense

You can't go one-on-one with an opponent you can't see coming. To counter an attacker's advantages in terms of flexibility and surprise, you need to develop a zone defense. In sports, a zone is a means of separating the field into areas of focused defense. The idea is that by creating separation, you can ensure that a threat either cannot physically reach an asset or that it encounters an increased defense when it does.

Establishing separation is at the heart of any effective defensive strategy, and the first step toward assuring security. To achieve it, build your game plan around the following:

- 1. Create zones by logically and physically separating services and assets from each other.**

Ex: Assets of one department should only be accessible to that department or group. All system accesses should be directly whitelisted (limited to a list of predetermined authorized types) through a switch and a firewall.

- 2. Create zones across your remote (vendor or cloud) accounts by using a separate login and secret sentence for each.**

Re-using passwords across vendors is the fastest and easiest way to get accounts compromised. Personal certificates and private key cryptography are much stronger than even secret sentences and should be used for administrative (root) access to external services. However, be sure to protect even those keys and certificates with a "secret sentence" — a password that is a complete sentence with capitalization and punctuation that means something to you so you'll remember it. For example, a secret sentence for Facebook might be, *I just wasted 2 hours on Facebook!* For your VoIP provider, it might be, *Boss says, "No more big bills."* complete with all the punctuation.

- 3. Create trust zones in the network where no system is directly accessible to another system.**

Ex: Desktops should not be able to connect to other desktops and network shares should be closed. Even if it's on the same network, no system should be able to reach another system unless you planned for it to. Have all desktops connect to a fileserver to store documents. Make sure all administrative access ports like SSH on servers or administrative web access on intranet servers are only be reachable by the administrator's system or, even better, manually on that server's keyboard if it's a local server. This is the network-level version of least privilege where only those who should access a particular document, printer, file server, or resource should be allowed to.

4. Create system zones in addition to people zones.

When you make zones of who can access what you are giving authorization to specific people and what they can do with their system. However, there is an inherent weakness in this type of zone: trust. Many types of attacks, like phishing attacks, use the trusts of a particular user to gain access to other systems without the user having any idea it's happening. You want to make sure that any resource accessed is done so by the person authorized to do so, and not secretly from their compromised system. One of the most common technologies to help you do this is CAPTCHA, which makes you prove you're human. In addition, it will reduce web comment SPAM and brute-force attacks (exhaustive attempts to guess passwords) on authentication systems.

5. Avoid all-in-one networked systems.

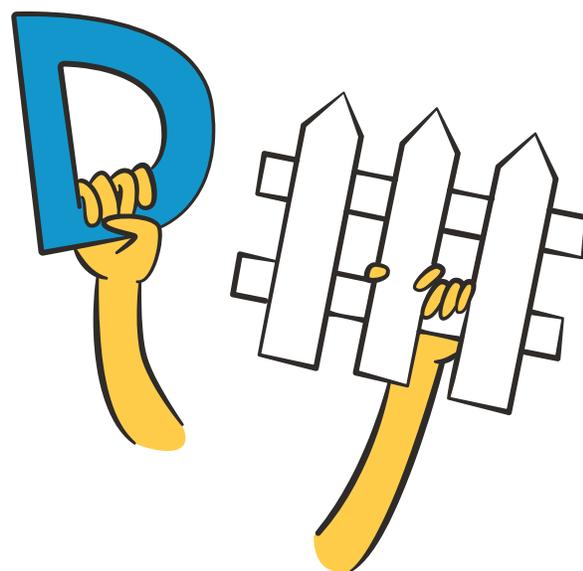
Examples are network access storage (NAS) + printer, or router + wi-fi. These systems are inherently weaker because they are more difficult to securely configure and more difficult to zone by filtering who is authorized to use them. If your router has wi-fi built in, disable it and instead use a wi-fi router in a special zone which cannot connect to internal systems.

6. Maintain a rigorous patching schedule for systems that are connected directly to the Internet.

While racing to patch should not be a primary defense, for Internet-facing services it's one of the few ways you can protect a server. For non-Internet-facing systems, you will want to make patching and other updates part of a regular maintenance schedule rather than automatically implementing them all the time. This will give you time to test the patches and updates on the standard system first, as well as create a routine in your network traffic that will help you identify malicious installs.

7. Create zones in your desktops, servers, and mobile devices that separate what can execute and what can read/write.

This allows for temp files to be created while denying temp files from executing in the case of malware. On desktops and mobile devices, whitelist specifically which applications may execute or use the network and deny the rest. Furthermore, exercise the principle of least privilege to ensure users don't get administrative or elevated privileges by default.



8. **Keep work and personal mobile devices separate.**

Apps have notoriously bad security, and each app on your mobile device is connected to every other app on that device. That makes the concept of zoning incredibly important. If your business requires the use of mobile devices then separate which can have personal apps and which can have work apps. There is technology to separate work and personal data on one physical device if you don't want to carry two devices.

9. **Create zones by using multiple web browsers to deal with web attacks.**

For example, you can keep one browser clean with no plug-ins and use it specifically for banking, vendor administration, and other critically confidential connections. Use another browser for online shopping. Use another browser for reading the news, surfing, and social networks (note: Do use ad blockers and privacy plug-ins on the browser for surfing to minimize exposure to malicious ads that force downloads of malware). You can also use a single browser with multiple profiles, however some browsers require a particular profile to be closed while another is open, and that can be a hassle.

10. **Zone your remote interactions.**

That means any remote access to your office, interactions with cloud services, administrating vendor accounts over the web, or sending emails. Your best protection for remote interactions is encryption. Use an encrypted VPN if the place you're sending or receiving from is not your place of work. Because emails are plain text and can be read along the route from one place to another you should use email encryption anytime you're emailing between remote offices or sending sensitive information.

11. **Use work times as part of your zoning.**

Shut down systems, routers, and wi-fi access points you don't need to keep running at the end of the day, weekends, and holidays. If you can't have staff support incident response for these things and be there to deal with emergencies then they should not be connected to the Internet during those times.

12. **Use blacklists if you can't whitelist or as an addition to whitelisting.**

A blacklist is a list of everything not allowed to enter or connect to a particular system. A whitelist, on the other hand, is a list of the things you allow. By using blacklists, you can deny entire categories of devices, programs, or service types if they aren't needed. Despite being weaker and easier to bypass than whitelists, blacklists are much easier to implement and maintain. This makes them practical as an additional form of separation.

For example, most antivirus software utilizes a blacklist that enumerates known bad malware to search for in downloads and installs. SPAM controls work mostly with blacklists. Most firewalls and routers can employ blacklists to deny access from countries where they don't do business. Specialized threat blacklists can also block known sites serving malware and launching attacks. Any of these can be employed as additional protection. Just keep in mind they can be shockingly easy for attackers to circumvent and therefore they should never be the main form of separation.

Apply Rehabilitation Tactics

As is frequently the case in sports, outcomes in security are often determined by conditioning that took place far in advance. Athletes don't show up to game day without putting in countless hours of practice first, and sporting franchises don't invest in star athletes without first ensuring they have the trainers, doctors, and coaches necessary to support them and keep them performing at their best.

Ask yourself: How rigorously has your security been tested? How many scenarios have you've prepared for? How quickly can you recover from setbacks and attacks?

Security is equal parts preparation and resiliency. To achieve that, you need to adjust your game plan so it includes regularly revisiting steps for what to do when something goes wrong.

Here are some rehabilitation tactics you should be sure to use:

1. **Set up a means to back up and restore systems, data, mobile devices, and desktops.**

Backups should be centralized, secured, and ideally encrypted. If your backups are encrypted, both off-site (cloud) and internally stored back-ups are acceptable. Just remember, anything backed up outside your network is no longer in your control. Then again, if you cannot afford to properly build and test a backup system then you're better off leaving control of such things to services that can. The key, however, is quick recovery, so test out restoring and make sure it happens quickly.

2. **Have tools handy to fully copy a drive for forensics investigations and recovery.**

There are both hardware and software technologies that can do this, some of which are certified to use in criminal investigations. If you have cyber insurance for your network, you may be required to use specific forensic software to make a claim.

3. **Keep shared data in central locations like a network access storage (NAS) server.**

That minimizes the amount of loss that occurs when a particular desktop fails. Standardized installs of desktops and daily-use devices along with nightly backups further shorten the time to full recovery. Being prepared for recovery will allow most compromised systems to be completely copied for forensics, wiped, and reinstalled to nearly full operation in under two hours.

4. **Back up everything – even your centralized data.**

It's the only way to assure a complete recovery. Set up all data services and file servers to be backed up and redundant with fall-back servers. This assures continuity and resilience so that server failure does not mean loss of service.

5. Have emergency contact numbers for vendor support.

If a forensics investigation uncovers why a particular attack was successful it may require immediate attention in the form of a patch, a configuration change, or both.

6. Consider investing in a distributed denial of service (DDoS) protection service.

This can be especially important if your business relies on customers having timely access to an online presence such as an online store. There are many of these and it's possible your hosting provider already offers this. However, you do need to make sure you know how much DDoS protection they can offer and perhaps invest in a vendor who specializes in it.



Use Your Home Field Advantage

The Internet is a hostile environment. That's the reason we go to so much trouble to make sure our networks are able to interact but still remain separated from it. However more than just creating a safe environments for our users we need to take things one step further and also make them hostile environments for attackers.

Creating an atmosphere and conditions that make it easy for you to thrive but difficult for your opponents – in sports this is what people refer to as home field advantage. Sometimes it can simply involve extra motivation and support from fans, but in some contexts there really are environmental factors involved. Some teams are better conditioned to perform on grass vs. synthetic fields. Others do better at high altitudes or in extreme heat or cold.

In cybersecurity, there are three primary “home field advantages” you should be striving to leverage: visibility, protocol, and process.

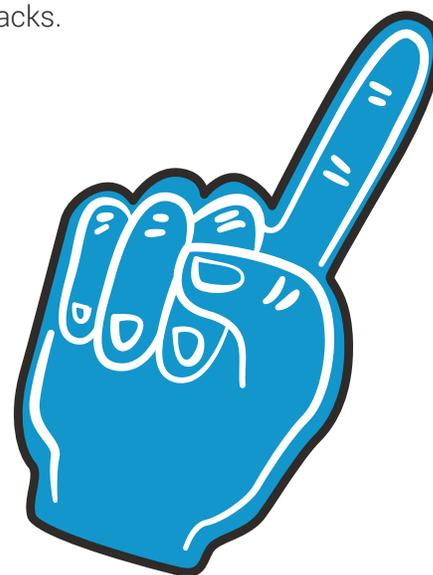
Do that and you can exploit the fact that, in order to do damage, attackers have to play the “away team” role. They have to come into your environment and contend with a network of systems you know better than anyone else.

Here's how to make the most of your home field advantages:

1. Know what's happening on your network.

This is probably your greatest home field advantage. To monitor your network for activity and have a clear picture of what's running at any time of day there are several technologies you can look into. Security information and event management (SIEM) products will consolidate log files from all your systems and real-time captures of network traffic. Intrusion Detection Systems (IDS), which are generally a blacklist technology, will monitor real-time network traffic and respond to some types of attacks.

Even without these technologies, however, tools like *tcpdump* and *Wireshark* will you give you more than enough information to understand what's running on your network and where it's going. That will help you at least see if your zone defense is working. As a network grows, you may want to look into behavioral analysis network tools to help automate sniffing out anomalies, because not all malicious activity is obvious.



2. **Know what should be on each default install of each hard drive, whether it's a desktop or a server.**

This allows you to recognize malware or non-standard software installs. If you prefer to use file integrity software you will be alerted to changes in various files and directories that can indicate malware or compromise. Integrity checking is most powerful on servers where it can immediately replace files placed by attackers.

3. **Change default settings.**

Your protocols are not just the types of packets that run on your network, but how you configure them to run. The attacker needs to learn what you're running, how it's connected to the rest of the network, and how it responds. By changing the default install and directory names, default logins and passwords on systems and devices, and default configurations such as the service ports of network devices and servers you can protect yourself from bot attacks which look for defaults. Simply moving the administrative port of SSH to a random, high number will keep it discreetly out of obvious reach while your network monitoring tools will notice a port scan and give you a chance to stop it.

4. **Change how your servers respond to queries.**

Attackers who footprint your network for a targeted attack will primarily be looking for what kinds of systems and applications you have. Changing how your servers respond to queries so that there are only positives and false positives will flood common attack tools with noise so they cannot tell if the tool's replies are true.

For example, something as simple as changing your web servers to respond to every request with a 200 even if it's not found or moved (error codes 404 and 302, respectively) can render common, automated web scraping and analysis tools mostly useless. You can tune your TCP responses also so every port queried responds to every SYN with an ACK. This is often most easily done with a port-forwarding firewall responding for the server, whether a server exists for that IP address or not. That technique makes a TCP port scan worthless. Of course, this will not stop an advanced attacker with access to better tools, but that's what your zone defense is for. Changing your defaults is how you make the pool of possibly successful attackers much smaller.

5. **Know what normal looks like.**

The way you do that is by knowing and understanding your employees, your vendors, your routines, your operating hours, and your policies. For example, if you know that no Microsoft Security center should be calling you to allow them to remotely inspect your system for malicious activity because you never paid for such a service then you'll recognize it as a social engineering or phishing attack and will be prepared to stop it quickly.

6. **Make your users part of the solution.**

By making sure all your employees are aware of what's normal, you can prevent a majority of fraud and phishing attacks. Employees who are aware of routines will notice quickly when a customer sends an email rather than calls. Changes in routine are a good indicator of possible attacks and employees are the first line of defense by reporting their suspicions. Making it routine for employees to escalate and document changes in processes can help create a forensic trail. Later, this can be correlated with patterns on your network.

You should also get in the habit of proactively talking to employees and asking how things are running. Complaints such as a noisy hard drive, a slow system, or strange messages can then be immediately investigated. If you are prepared to perform quick recoveries, a system that is acting suspicious can be quickly wiped and reinstalled.

Part 3: Looking Downfield

Despite the sports analogy, let's be clear, cybersecurity isn't something you dabble in. There's no bush league cybersecurity. It's not a game. Losers are real victims who incur real and sometimes catastrophic losses. Even winning is just a fleeting moment that is gone as quickly as it came.

Cybersecurity is hard because we don't know all of the possible vulnerabilities we have or all of the possible threats there may be. Even if we could, they change too frequently for us to maintain specific defenses.

That's because the environment we work in is changing all the time. New technologies, new business models, new services, and new communication channels make it extremely difficult to secure it all. Furthermore, this competition against attackers will last indefinitely. That means your overall strategy has to be winning not just this season but every season after that.

To do that you need to keep your players in shape, steadily improve your equipment, maintain a healthy environment, and employ the right tactics to stay in the game. In this section, we'll cover how.

Training

All employees need to understand how cybersecurity affects their personal day-to-day role in the company, and they need to be trained in situational awareness both on and off the computer.

- **Teach all employees how they can be manipulated and fooled both in person and online.**

There's an infinite number of variations that an attack can take but a finite number of ways a person is vulnerable to fraud and manipulation. Rather than expect employees to be able to identify all manner of constantly shifting threats, instead teach them how to react securely when one of their vulnerabilities is probed (ex: when they're asked for sensitive information).

- **Make it easy for employees to talk about their security or privacy concerns.**

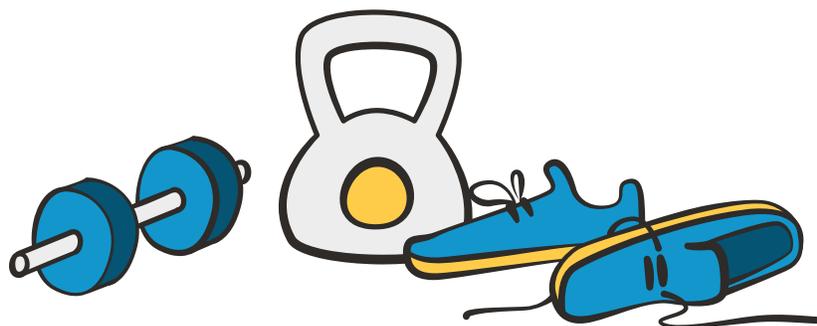
Employees are a company's best anomaly detection engine. Make sure they will be able to voice their doubts and unusual activity before those concerns grow into big problems.

- **Really know your systems.**

Anyone working in IT or cybersecurity should be well versed in how all of the current software and systems work inside the organization. It's not enough to be certified or experienced in the brand of technology. You have to know how it works in your organization. You can't secure anything if you don't know what it does and how it works in your environment. Bring in a coach that will teach you and others security in the context of your operations.

- **Understand how to apply the basics.**

All cybersecurity personnel should be well versed in operational security fundamentals as **outlined in the OSSTMM** which they can apply anywhere from physical to cyber anything. It's not enough for them to say they read it, have them map your business processes into its controls and limitations as shown in the OSSTMM to see exactly how big your attack surface is.



Exercises

Knowing how to swim doesn't mean anything when the tsunami hits. To stay above hostile waters you need to train regularly on how to react when things go wrong. Only with exercises can you assure that despite fear, confusion, or fatigue, the default reaction is the secure one.

- **Create an incident response plan and drill it.**

Create an emergency checklist employees can use and keep practicing walking through it until everyone is clear on how they should react. Include all new hires in the drills from their first day.

- **Get employees used to dealing with attacks.**

Plan regular security exercises designed to manipulate employees such as mock phishing attacks, social engineering in person and on the phone, and fake malware activity.

- **Give mandatory security challenges and puzzles.**

These should take no more than a couple minutes to complete and are designed to be done without taking employees completely out of their day-to-day tasks. This trains employees to think security while doing their normal activities since nobody has the luxury to stop working during real attacks.

Equipment

In many sports, being the better athlete doesn't guarantee a win on its own. The difference between first and second place can often come down to the equipment. New materials, new technology, and new designs can give you a critical advantage.

- **Make the most of your tech.**

In cybersecurity, having better routers increases response times, better processors allow for stronger encryption protocols, and more elastic monitoring solutions reduce the need to spread out resources.

- **Consider the cloud.**

Cloud-based services can provide you with additional functionality you don't have to build or manage on your own. There's a trade-off in terms of control and self-sufficiency, of course, but the added capabilities can allow you to do more with less.

- **Even when you can't allocate resources on new equipment, you need to maintain the old.**

Sometimes just upgrading components like RAM and hard disks is enough to make a difference.

- **Keep your systems running lean.**

Stick to necessary software as much as possible, minimizing the memory resident and memory-hungry software that can slowly grind a system to a halt.

Environment

Some athletes compete on clay, some on dirt, some on grass, and others on artificial surfaces like artificial turf or asphalt. What they all have in common is that they've honed their game to adapt to that environment and they've cultivated a home field advantage by learning how to outcompete others on it accordingly. You need to do the same by getting to know your own environment by actively maintaining it and understanding even the littlest changes.

- **Know what “normal” looks like.**

Make a routine of examining the protocols on the network, the systems that interact with each other, the ways the employees use their desktops, and how mobile devices operate in this environment. Fire up a packet sniffer and watch live traffic in different segments. Make sure you know what it all is and whether it should even be there. If you can get a professional tool for constantly monitoring traffic, like a SIEM, even better. Then track down those anomalies.

- **Remember. Not all software needs to be updated.**

You should always update if a security patch is necessary and you have no other means of controlling the vulnerability. However, that requires you have the people and time to investigate that. If the updates are for new functionality only, on the other hand, consider whether you really need this new functionality. Many a process has been broken and many a file has been lost because an application or system update made changes you didn't need or anticipate. As any coach will tell you, if it's not broken, don't fix it. So have a process in place to pick and choose which updates get installed.

- **Make rounds and talk to employees.**

Get to know what they need to do their jobs, how they interact with third party vendor services, and what software they use regularly. People develop routines and habits at work. They are your best source for knowing when something outside your basic control like cloud services and vendor extranets are not behaving like normal.

Forget Strategy, Choose Your Tactics

A strategy is an integral part of any modern business plan. So what exactly is a cybersecurity strategy? A cybersecurity strategy is a plan with a set of goals and objectives to achieve cybersecurity as a result.

People who are into selling cybersecurity strategies like to say it also includes specifics on tools and metrics. But that's really just a trick of adding tactics to the strategy so it doesn't sound so useless.

Yes, useless. Fun fact for you — a cybersecurity strategy is useless. The truth is if you don't have one for your business it's because you've inherently got one already. You've never bothered to formally document it because it's so obvious. Like how you don't have a formal not dying strategy. If you were to have a formal cybersecurity strategy it would likely say you don't want threats of any sort affecting your assets of any sort now or in the future. Which is obvious.

So if it's useless, why is there such a focus on a cybersecurity strategy? Because tactics are hard.

It's easier (and safer) to make a cybersecurity strategy sound like something important despite meaning nothing than it is to choose and implement tactics that work. You look better longer, too, because whereas a cybersecurity strategy can go on meaning nothing a really long time tactics that mean nothing get noticed right away.

Cybersecurity tactics, meanwhile, are where the rubber meets the road. They are the bat striking the ball. They are literally the packets smacking the server. They are the way you “do the thing you do to the things you have” to achieve cybersecurity. And that's hard to plan out. That said, here are a few steps to point you in the right direction:

- **Draw out the interactions and the separations between your systems.**

This should be based on the packet activity you find on the network. It's like making a hybrid physical and logical network map with arrows of interactions based on protocol activity. Determine how anything that should be separated or controlled. Voila, that's you applying tactics!

- **List all of your network processes.**

This includes server backups, server administration, remote desktop support services, etc. Know exactly what systems and people they can interact with, then determine what they should be interacting with. How you control that authorization is you applying tactics.

- **Do the same for wireless, physical room and asset access, and telephone systems.**

Determine which tactics you need to apply to assure control.

- **Now take a step back.**

Make sure that all of the tactics you chose fit with the overall company strategy and resources and that workflow is not hampered.

Learn to Work with Non-Technical Colleagues

Humans are social animals. The majority of us like being liked, like belonging to a group or a team, like standing up for a cause, and like being part of a community. Or even if we don't "like" it doesn't mean we want to be pushed out of it, either. The problem is just because we like it doesn't mean we're good at it. A lack of communication with the people holding the resources will greatly affect your ability to build the security that's needed. Here are some tips for making communication run smoother:

- **Don't assume because it makes sense to you that it makes sense to everyone.**

It's normal for people not to like change. Therefore you need to consider this hurdle anytime you're proposing change and prepare for it by showing that change is the new normal. After all, the criminal hackers entering organizations like yours have had plenty of success, and they change tools and techniques all the time.

- **Communicate with your coworkers or your boss according to their capabilities.**

If they are tech savvy, don't talk down to them. If they aren't technical, don't go to them with tech-heavy reasoning.

- **Think about the money before you talk.**

Your company is in business to make money. Show value. Provide ways to show that additional security can replace some of the things you are currently doing. Or if that's not possible, show how various solutions can reduce downtime, add quality, or improve efficiency.

- **Don't waste their time.**

Don't let them even feel for a moment that you're wasting their time. That means being prepared and polished.

- **Never say, "I told you so."**

Don't bring up that time your suggestion got ignored and something bad happened. Don't make it seem like you did them a favor or that you expect something for your brilliance and insight. Start from zero each time.

The Big Picture

In cybersecurity, you're dealing with conflicting information from authorities struggling themselves to understand what makes or defines "good" security. Some of the most common questions leave most security professionals simply guessing as to what's the right answer: Is it more secure to harden servers or use a firewall? When do you need two-factor authentication? Which is better security, certificates or passwords? Do reverse proxies actually provide more security?

That said, cybersecurity is also maturing as a field. Every year, there's less misinformation and more and more people trying to come to terms with the fact that they were at least a little wrong last year. But humility is not for everyone, and security is a humbling experience for everyone. It's like in sports how you can keep thinking it was a great game right up until the point when you wondering how you lost. Things don't tend to just gradually grow bad — they suddenly do, surprisingly so, from one breath to the next, the same way you go from running like a gazelle to sliding across the ground with no idea why you fell.

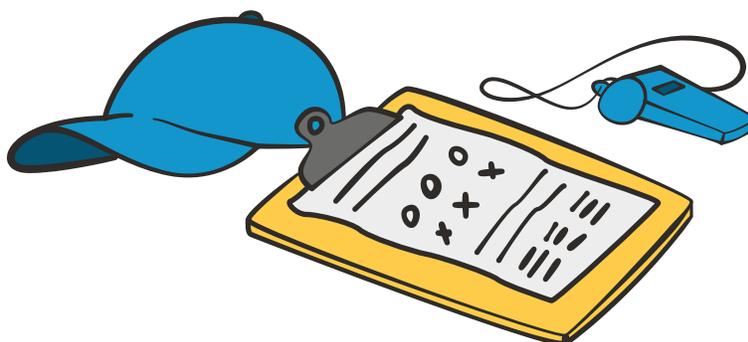
Luckily, the online cybersecurity community has more advice than you ever need — even if it does conflict a lot. And one of the great things about such a huge, helpful, self-interested community of humbled people is that they really want to help. But you need to be careful with that if you want to really set yourself up for long-term success.

What happens is that by relying on the cybersecurity community for your answers you will ultimately get mostly the answers that allow the security community, especially vendors to profit. This skews the directions future security research takes. It skews the tools that security vendors make and sell. Most of all, it skews the knowledge you need to know in order to improve your own security.

What you'll eventually learn is that good security professionals tell you what you want to know. But great security professionals tell you what you need to know. You'll know when it's the latter because it will frustrate you and seem like a pain in the ass and leave you wondering if you can't just buy and install some product. You can. But without putting the work behind any product you install to make it fit your environment and your processes then you won't fix the problem. More likely, you will create a set of new ones.

The cybersecurity field hasn't matured enough to know what's right all the time. It has a problem of letting go of what isn't working. It still tries to base success on effort rather than security. So the first thing you need to do to improve yourself is to stop repeating things like "Everyone gets hacked eventually" and "If a hacker really wants in they'll get in" and "Security is a process." Because if our humbling experiences have told us anything, it's that security isn't a slogan or a comforting phrase. It's the toughest riddle you'll ever have to solve before the Troll comes out from under the bridge and eats you. And every riddle has a different answer every time. It's constantly changing based on the environment you're in.

So as you set out to win in the cybersecurity field remember that the security community is a resource and not an answer, just like Wikipedia is a resource and not a term paper. What you get from it will rarely fit your needs as-is. You still need to figure out how to answer your own riddle, and that takes knowing your environment, your employees, and how it all works together (aka the Big Picture). You need to know where the interactions are, what resources are being used and from where, as well as who has authorized access to what. And you need to do that constantly because every second, the riddle changes a little bit. Or else before you know it, it's changed a lot and you're not ready for what happens next.





At Barkly, we believe security shouldn't have to be difficult to understand or implement. That's why we support projects like this one and why we're dedicated to providing companies like yours strong endpoint protection that's fast, affordable, and easy-to-use.

Learn more at www.barkly.com.

ISECOM

The Institute for Security and Open Methodologies (ISECOM) is a non-profit, open research organization focused on all things related to security and hacking. ISECOM created and maintains the Open Source Security Testing Methodology Manual (OSSTMM) and Hacker Highschool designed to teach cybersecurity to teens.

Learn more at www.isecom.org.