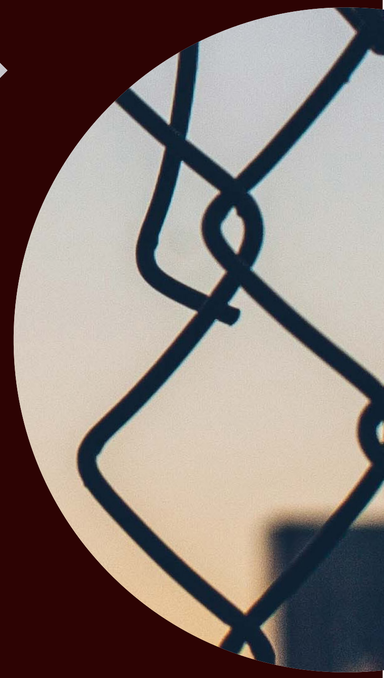
Ebook

WITH secure



The value of impediments
How to be more trouble than you're worth

Contents

Introduction

Effective deterrents prevent unwanted activity by threatening negative consequences; the threat of being caught, arrested, and sentenced is generally the best deterrence against crime. Unfortunately, effective deterrents do not exist in the world of cyber security.

Organizations (and regulatory bodies and law enforcement agencies) have very few ways of punishing or otherwise harming cyber attackers. The likelihood of catching cyber criminals is very low, and it is also very difficult to prosecute them because they often operate globally.

Concepts like ‘hacking back’ (legalized intrusive action against cyber criminals by private organizations) are regularly discussed, but they have so far always been rejected due to concerns around transparency, the potential for misattribution, and the potential for collateral damage.

What can we do?

Where deterring attackers is impossible or impractical, organizations can turn to impediments.

You cannot expect to actively punish threat actors who target you. But you can design your defenses so that you are more trouble than you are worth, making yourself an unattractive cost/benefit equation in the eyes of an opportunistic threat actor.

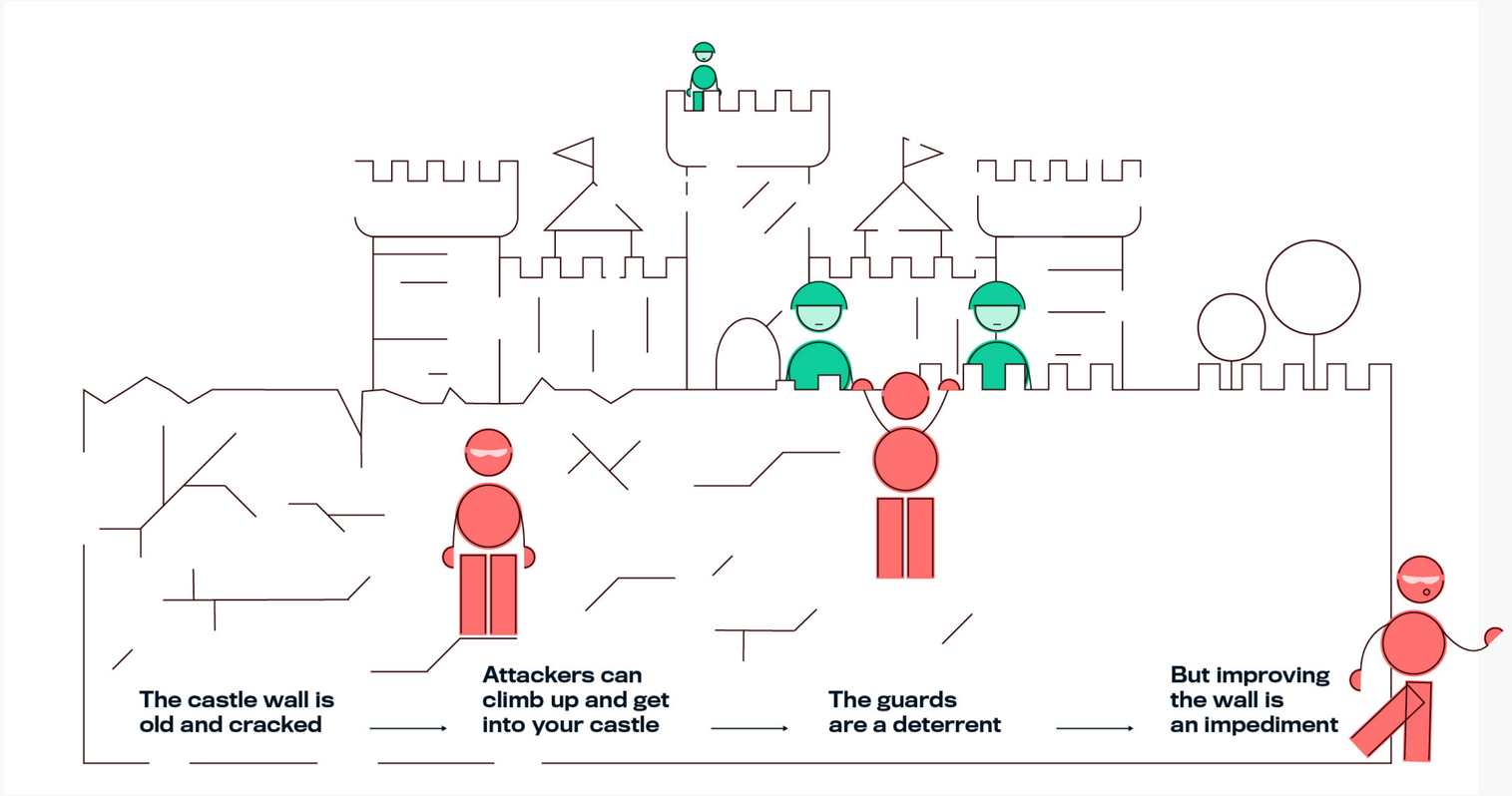
Imagine your organization is a castle surrounded by a tall stone wall. The wall is old and has many places where the stone has broken or the mortar has fallen away. Its surface is so uneven that an attacker could easily climb over and sneak into your castle.

In this scenario, a deterrent would be armed guards stationed on the top of the wall, ready to capture any attacker who reached the top.

But that attacker could also be impeded by improvements to the wall. If you filled in the cracks and holes, the wall would be much harder for the attacker to climb. It may even become so difficult that the attacker gives up and goes away.

Impediments are designed to waste attackers' time and money. Effective impediments buy time so that defenders can detect and contain the attacker and may frustrate the attacker so that they abandon their activities.

Examples of types of impediments include simple layers of defense, which an attacker must spend resources to penetrate; withholding information that would make an attack easier; and collaborating with other organizations and individuals to share knowledge and reduce the effectiveness of known attack paths.



Get the basics right

Some of the most important impediments to a cyber attack are also some of the easiest and cheapest to implement - within the reach of every organization. Practical policies that follow current best practice around passwords, authentication, restrictions, education, and physical security are the foundation of cyber security, and although most people understand these basics, they are still often neglected.

Passwords

Weak passwords, or weakly-secured password lists, are like gold to attackers. If a threat actor can find or decode your passwords, they save significant time and effort. Robust password policies are therefore one of the most fundamental and universal impediments to attackers.

For key assets, it can be useful to use tools like enterprise privileged access management solutions that can manage passwords for you. For example, it can regularly create new temporary passwords so that, even if an attacker found old passwords stored on the servers, they'd be useless.

We recommend that organizations mandate long passwords (or passphrases), but no complexity requirements. Increasing complexity (adding in numbers and symbols, for example) does make passwords harder to break, but passwords should be memorable. If you remove complexity requirements, you can require longer passwords that employees will actually be able to remember (without writing them down). Password length is the main factor in increased security: we recommend a 20-character minimum.

Complexity requirements can also bring a false sense of security. For example, if you require a capital letter, nine out of 10 people will capitalize the first letter of the word. When this is so predictable, security is not really increased.

Story from a red teamer

“The quickest engagement I can remember was one where we found all the target’s passwords on the file share in a password manager. The file was protected by a password, but it was very short and did not take long to crack, and after that we had all the passwords to the other areas of the network, and therefore all the access we needed. We found that file within two days and cracked the protection overnight.

Of course, we paused the engagement there to highlight the risk to our client so that it could be controlled. But if we were malicious attackers, we could have fully penetrated that environment in just a few days.”

~ WithSecure™ red team member

Authenticate

Authentication is a major impediment to attackers. If, for example, your organization uses a VPN, but you do not have to authenticate your identity to use it, an attacker can get access to the network simply by having one of the organization's devices. If you require authentication, the attacker will have to do more work to get the same result. Multi-factor authentication is best, but any kind of authentication is better than nothing.

Educate employees, and restrict them

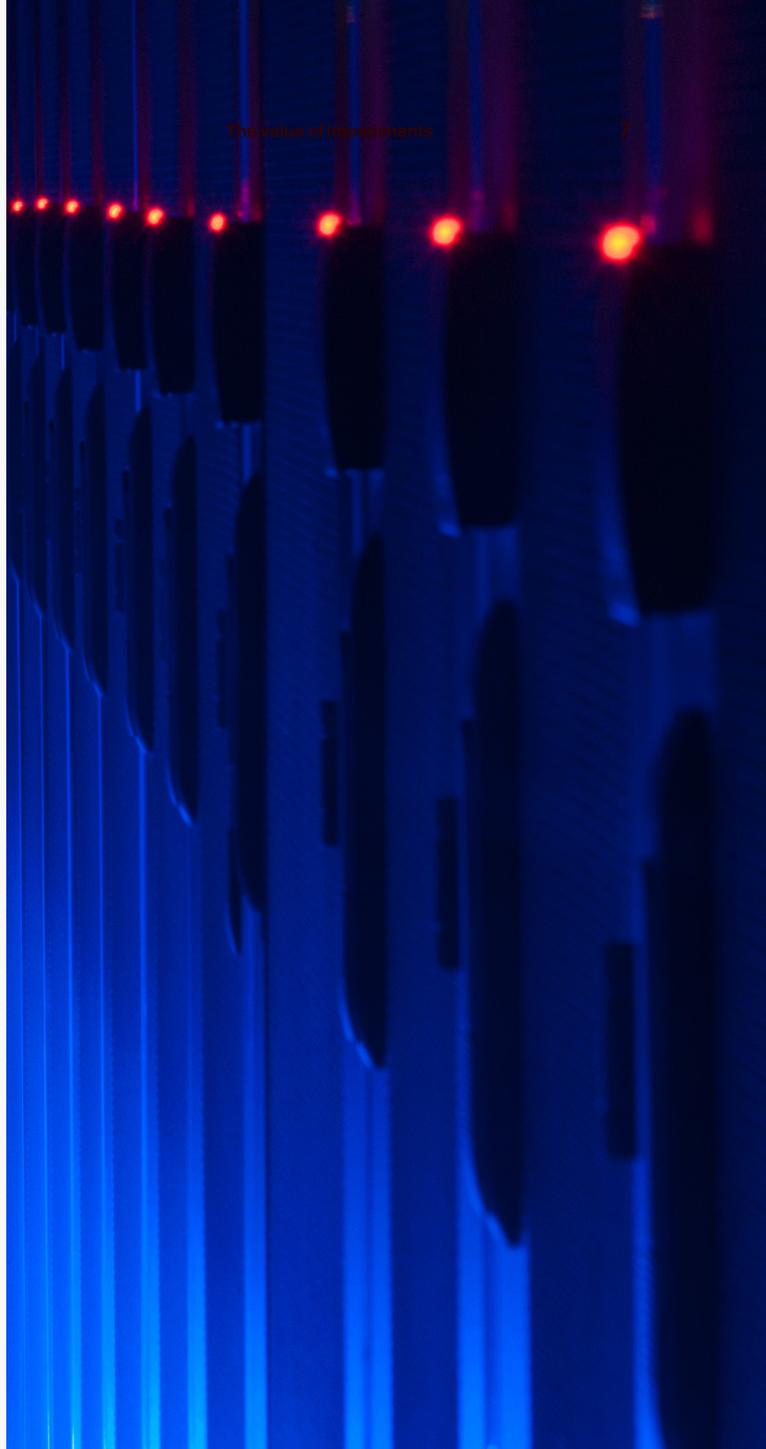
Users will do what it simple for them. For example, they will put documents in a shared drive because it is simpler than assigning access to individuals. They will fulfil minimum password requirements, but will typically not exceed them.

You can and should educate people so that they understand why, for example, passwords and access controls are necessary, and how to recognize a phishing attempt. This will prevent security holes and lapses. But unfortunately you cannot stop anyone from ever clicking on a phishing email – one will eventually get through. That's why it is important to build in controls, like controlling who has admin rights in certain areas, to prevent actions that may have unintended security consequences.

Physical security

Remember to consider physical security as a part of cyber security. Many cyber defenses can be sidestepped if an attacker can enter your offices and steal a device.

Make sure that your offices and other on-premise locations are equipped with security basics like photo-ID cards and automatic-lock doors. Design robust physical security practices and ensure that your employees understand them and are compliant.



Increase friction

The best way to defeat security controls is to simply step around them. Forcing the attacker to interact will make it harder for them to progress and make it easier for the defenders to detect and contain the attack.

The two main elements of increasing friction are:

- control access
- separate elements of the network.

Control access

In general, users should have the minimum amount of access necessary to do their jobs. This will be annoying for employees, who will experience delays when they need to request access to new areas, such as specific SharePoint sites. But it's a necessary evil, because universal access is dangerous.

Attackers will often impersonate users, such as by using certain login details that they have found or decoded. If every user has universal access to your system, then the attacker only has to impersonate one user throughout the engagement. This is difficult to detect. If, however, the attacker has to leapfrog between accounts to access different areas of the network, they are much more likely to trigger alerts or otherwise be detected. Also, this will probably increase the length of the engagement, giving you more time for defense.

Separate elements of the network

Attackers can find and access things easily in networks that are wide open and well connected. If networks are properly segmented, attackers cannot always directly access their targets. Instead, they have to interact with more hosts or security controls along the way.

Attackers must often pivot through different axes, for example, from the account of a user to a host. If that next step only has access to a limited additional attack service, then even more pivots will be needed, increasing the opportunity for detection or prevention and increasing expense for the attacker all the time.

Remember to also maintain a good understanding of all the assets in your inventory. Blind spots and shadow IT are weak spots in your defense.

Story from an incident responder

I remember one incident that was caused by shadow IT. A former employee in the IT department deployed his own servers and made them part of the network without telling anyone, and then left the company. That was a massive security risk because those servers were not included in any of the asset lists, and so they were not being maintained at all.

~ WithSecure™ incident responder

Manage assets

Aside from designing your network to increase friction, it is important to manage your assets properly to impede attackers.

Patch known vulnerabilities

Make attackers' jobs more difficult by patching known vulnerabilities in all your assets. Doing so will deny attackers of an easy foothold into your environment.

Story from a red teamer

"We had a case where we used a new vulnerability to get a foothold on some systems. That client was aware of the vulnerability and tried to patch it, but apparently did not include all their assets in their patching procedures."

~ WithSecure™ red team member

A vulnerability patching process is useless without a thorough understanding of the assets in your environment (both on and within the attack surface). At a minimum, you should have a complete list of assets. Ideally, these would also be prioritized in order of patching urgency, should a vulnerability become known.

Minimize attack surface

An 'attack surface' refers to an organization's externally facing assets that could be targeted by an attacker aiming to gain unauthorized access to resources or to exfiltrate sensitive data. Common elements of a modern attack surface include externally facing websites and services, cloud hosting providers, third parties, and content delivery networks, as well as information assets such as source code, configurations, and databases stored in buckets or code repositories.

Threat actors targeting a specific organization will map the attack surface to determine the easiest routes into the environment. The larger the attack surface, the easier it is for the threat actor to find an entry point. Threat actors choosing which of two target organizations to attack will choose the one with the largest attack surface, all else being equal.

Minimizing your attack surface as far as possible is therefore an effective impediment against attackers, who may need to spend expend much more effort to breach a well-managed attack surface then they would for a larger, uncontrolled one.

It is vital that you remember to secure or protect any assets that remain in the attack surface, as minimizing the attack surface is ineffective if the resulting assets are easy targets for attackers. Attack surface management shouldn't be relied upon as a complete solution: much more should be considered when assessing perimeter risks, such as understanding how the organization might be targeted by particular threat actors, as well as which assets are considered critical and most at risk.

Read this for more information about attack surfaces and to learn about our external attack surface management service.

Control open-source intelligence

Every organization generates publicly accessible information, which is often uncontrolled. It comes from sources like the organization's website, marketing campaigns, social media, independent news reports, job adverts, public reviews of the company from former employees, and so on. This type of information is known as open-source intelligence (OSINT).

Threat actors can learn a surprising amount about an organization and how it might be successfully attacked through OSINT. For example, the job adverts for the security team in a specific organization can give attackers huge insight into how security is managed there; if the advert specifies that a candidate must be proficient in a specific endpoint detection and response technology, the threat actor then knows that it is an element of that organization's cyber security.

Controlling OSINT is therefore a valuable, if difficult, task. If you can limit or control how much OSINT is available, threat actors have to work harder to understand your environment and defenses and, if they do attack, will be more likely to get caught by defenses that they did not know to prepare for.

Story from an incident responder

"I remember an attack by a state actor. We found that they were monitoring certain users' email boxes. We googled these users and immediately found their profiles on the company webpage, with a little bio that explained what projects they were working on. That public information put a giant target on the back of those employees.

~ WithSecure™ incident responder

Unlike with attack surface management, you should not necessarily aim to reduce OSINT to a minimum. Effective OSINT control is about making conscious, informed choices about what information will be valuable to threat actors.

For example, an organization that has won a cloud security award may want to publicize that information, but they should consider that some threat actors will see it and want to test their skills against their top-tier security system.

It is worth defining policies around the types of information that should be shared publicly and educating employees about the dangers of uncontrolled OSINT.

Gather and share information about attackers

Threat actors are innovative. New attack techniques are constantly emerging, which makes it difficult for defenders to prevent and mitigate damage.

However, sharing information about these techniques—whenever possible—is a significant nuisance to threat actors. When this happens, their techniques become much less effective as organizations work out how to defend against them. Threat actors must then spend time developing new techniques, which is time that cannot be spent in more lucrative adversarial activity.

You can share information about attackers and attacks online, such as on the VirusTotal site. Remember, though, that these sites are often monitored by attackers. Uploading information about a new technique as it is being used in your environment can alert attackers to the fact that they have been discovered. It is better to wait to share information until after the attacker has been contained or ejected.

Some organizations share details about attacks in private channels, which has the advantage of not alerting the attackers that they have been detected.

Honeypots

A honeypot is a trap designed to lure in attackers. It is essentially a decoy, and in cyber security often takes the form of an entire computer system, including realistic activity and data. The honeypot will often be ‘baited’ so it becomes tempting target, either by loading it with fake but appealing assets (like billing information) or by worsening its security posture slightly (such as by securing it with weak passwords). You can also create honeypot accounts, which are cheaper and easier to deploy, maintain, and monitor.

Honeypots are useful for many reasons, not least because they can prevent attackers from acting on your legitimate systems. They can also enable the detection of attackers who are using legitimate credentials and masking their activity by using as little malware as possible, because any activity in a honeypot is suspicious.

Critically, though, when hackers attack the honeypot, the organization gets valuable information about how attacks may be conducted, what triggers to monitor, what cyber criminals are most interested in, and so on.

Build a reputation

You can build a reputation as an organization that regularly or consistently shares information about attackers and attack paths, which may make threat actors think twice about spending their resources on you.

Summary of recommendations

You can take many actions, even in smaller organizations, to impede attackers. These include, but are not limited to:

- implementing policies based on current best practice to manage the basics of cyber security, including passwords, user authentication, employee training, and physical security
- increasing the friction between the attacker and your security controls
- managing assets so that there are fewer opportunities for attackers
- controlling OSINT
- gathering and sharing information about attackers.

Remember that these techniques, although effective and useful, cannot replace a complete cyber security solution. You aways need to be prepared to mitigate attacks that penetrate the outer layers of your defense.

Visit our website to learn more about holistic cyber security.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure