SolCyber

Security that matters:

Where to focus your dollars and time to make impactful improvements to your security posture

SolCyber

Several years ago, the security landscape looked drastically different. Unless you were a company with sensitive data to protect, security wasn't really on your radar. For most small and mid-sized businesses (SMBs), cybersecurity involved installing antivirus software, (maybe) patching your systems, and performing general cyber hygiene.

That's because in the private sector, most hackers would break into systems, steal valuable data, then sell it for a profit. But now, hackers break into your systems, steal private or embarrassing data, lock it up, and force you to pay to regain access to your own systems or data to keep the thieves from posting your most private data to the internet.

That means every business, regardless of size or the types of data stored, is susceptible to an expensive ransomware attack.

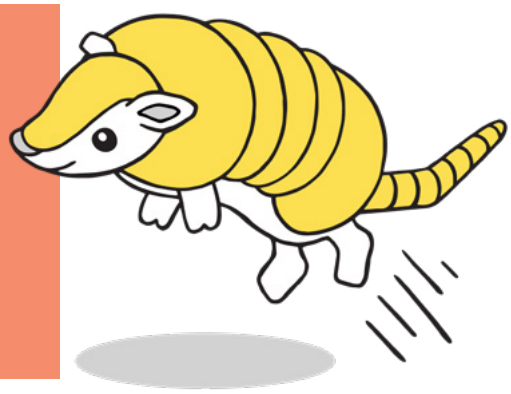
The way hackers break into systems to conduct this attack is also different from the way it used to be, which is why businesses need to invest in security tools and practices that look for bad behaviors and techniques rather than tools that simply scan for known malicious software. It's a fine detail, but an incredibly important one for companies focused on risk reduction. We like to say, "instead of looking for people wearing ski masks inside the bank, look outside for a vehicle full of people driving a stolen car with guns and a bunch of empty pillowcases."

The plethora of security software, tools, and frameworks is overwhelming and never ending. Navigating the world of cybersecurity can be intimidating for any person new to it and even for technology experts. Where do you put your money, time, and effort to reduce risk? Many frameworks start with asset inventory, but is this really the best place to begin if you have no security framework? How long will it take you to get proficient at asset management? Furthermore, how will world-class asset management reduce risks from social engineering? The reality is: it won't, that's how attackers get a foothold in companies every day.

So rather than starting with a framework, there are a few things you can do right now that will immediately and dramatically reduce the likelihood of a security compromise.

These are the five areas in which businesses need to invest and become proficient when dealing with modern cybersecurity:

- **Phishing protection**
- **Endpoint detection and response**
- **Patching**
- **Deception tactics**
- **Managed detection and response**



When working together, these five defenses can provide real protection and significantly improve your security posture. Anything less and your business is vulnerable. Anything more and you may be overpaying for products and services that ultimately won't move the needle. Worse yet, until you have these five simple things mastered, anything new is likely to distract you from mastering the techniques and the signals they produce. This combination of tools, techniques, and services make up what we like to call the "security that matters."

01.

INVEST IN A PHISHING TRAINING PROGRAM

Roughly 80 percent of data breaches start with phishing or use phishing to advance the effort, so this isn't an area to skimp on when it comes to protection. Companies large and small should be phenomenally good at resisting phishing attacks, but that's often easier said than done. Phishing attacks prey on human fear or curiosity, and no amount of email protection software can keep your employees from clicking on a bad link.

To truly protect your organization from phishing attacks, you need to invest in a three-step approach that includes robust training, testing, and the reporting of discovered phishing attacks. All three are equally important.

1. Make training engaging and customized

Training is perhaps the most difficult step as many simple computer-based, click-through programs aren't effective. Let's be honest, have you ever taken one of these trainings and given it your full attention? Yeah, we haven't either. And yet, many companies use the same boring training attempting to prevent a multi-million-dollar mistake! An interactive, consistent, and iterative phishing detection training program that's customized to your teams will be far more effective at creating real behavioral change.

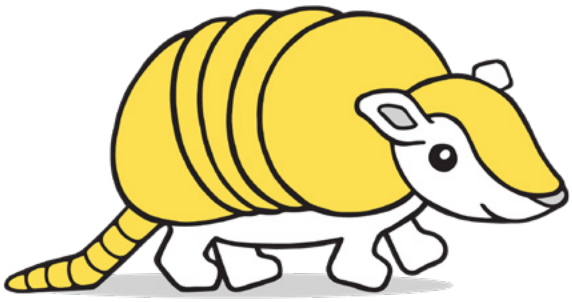
Focus on the right areas

When it comes to assembling your initial training, don't circulate the latest scam you saw on the news and focus on the traits of that particular attack. Too often, companies focus on the most recent phishing attack, but this is a lagging indicator, and these warnings to staff can do more damage than good.

Here's a scenario for you. On Monday, you see a phishing attack with a FedEx theme, so you warn all your people about a FedEx attack. Everyone is immediately skeptical of any email that looks like it comes from FedEx. On Tuesday more phishing emails come in, and they have an iCloud theme. Your people are looking for a FedEx-themed email, so they don't think twice about the iCloud email and fall victim to that phishing attack. You then warn teams about an iCloud email and the cycle continues.

By concentrating on the last attack, you're not protecting your organization from the next attack.

Instead, focus your training on the techniques that phishers use to trick their prey. For instance, make sure employees understand that phishers may pose as another person or company, ask you to click on a convincing-looking link, and send messages that convey a sense of urgency. By knowing the red flags of a phishing email, your employees are more likely to resist the temptation to click, regardless of the sender. Only then can your employees become phenomenal phishing detectors.



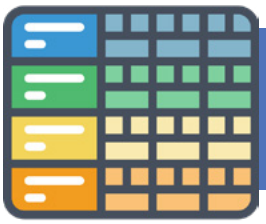
Employees should also learn that clicking the link alone won't always be enough for a hacker to break in — the employee also needs to open a file or enter a username and password. Knowing this gives employees one more opportunity to avoid a scam and do the right thing. Too many phishing training programs stop with the first click or the opening of an attachment. But most phishing attacks require more steps to be successful. By ending the learning process early, your training misses one, two, or even three more opportunities to make your people the best phishing detectors possible. So, when looking at existing testing tools, or building your own, make sure clicking on a bad link isn't the point of failure. Allow employees to click a link and continue with the phishing process to teach them to look for additional clues that something is wrong —actions that could help them avoid disaster and salvage the situation in real-life scenarios.

2. Test the effectiveness of your efforts

Once you've conducted your initial training sessions, you need regular testing to see if the training stuck and to determine how resilient your organization is. Send phishing emails at least once a month and track how employees perform over time. It's important to note that these tests shouldn't be viewed as a means of identifying and punishing employees who fail your test. This is merely a performance metric to determine the effectiveness of your training program and measure the overall resiliency of your organization. As you begin looking at scores, make adjustments to your training modules and then see how those changes affect the overall outcome.

If an employee fails your test — and many will — the failure should be exposed to the employee with a micro training opportunity. (Remember the 'ole saying, "Strike while the iron is hot"?) To ensure the micro-training isn't seen as a punishment for failing the test, use positive and encouraging language that clearly identifies what they missed and how they can succeed the next time around.

By testing employees and measuring performance, you'll have hard numbers and KPIs to bring to your board or leadership team that prove the effectiveness of your security program.



These numbers can also be put into a leaderboard to gamify training and testing.

Find ways to encourage departments or offices to compete for the top spot (or avoid sitting in the bottom half of performers). The competition will get people excited about cybersecurity and phishing training rather than seeing it as another box to check.

3. Give employees the opportunity to report scams

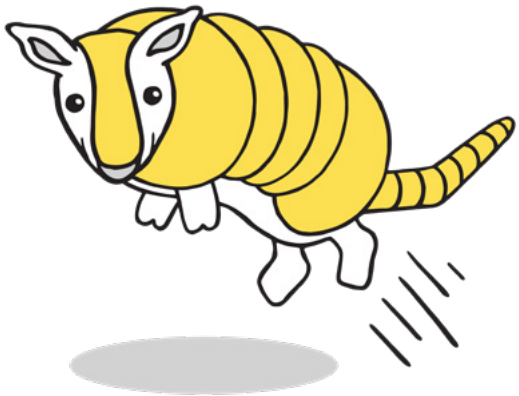
No matter how great your training sessions are or how competitive teams become, your employees are still human, and humans are flawed. Although you can aim for high success rates on your tests, someone will inevitably click on a phishing email and take the wrong action. It happens in every organization, and the best you can do is be ready when it does.

Make sure employees have a means of reporting phishing scams so you can react as quickly as possible. Once someone reports a phishing email; identify the indicators of compromise, determine who else received the email, and try to de-risk the email so additional people can't fall victim to it. Next, determine who else fell victim to the attack, what the attack does, and unwind the damage. Ideally, this process will be highly automated, but it still needs to be triggered by a human reporting the phishing email.

If you don't give employees the ability to report phishing emails, you can't begin this process. Your people will become the most valuable phishing prevention solution you have. For this reason, having a high reporting rate is just as important as having fewer people fall victim to the attack.

If you can see it, you can de-risk it.

If the attack is never reported, you miss a huge opportunity to de-risk one of the most effective tools hackers have in their arsenal.



02.

MOVE BEYOND ANTIVIRUS SOFTWARE WITH ENDPOINT DETECTION AND RESPONSE TECHNOLOGY

Endpoints are frequently where hackers get a foothold in your environment, so it's essential to have adequate security measures in place to stop nefarious activity from occurring here. While antivirus software will notify you when known malware is found on a computer, that's where the software's usefulness ends. Plus, even the most unsophisticated attackers can easily hide their malware from standard antivirus. The bottom line is that your security team still needs to go in and verify that the activity was, in fact, malicious and respond to the threat; i.e. evicting the attacker from your environment.

Pay now, save later

The price tag on EDR technology is higher than that of antivirus software, but it's well worth the investment when you realize the other ways these solutions help.

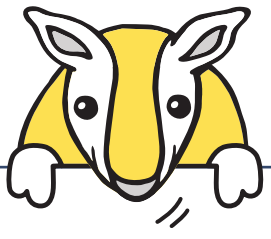
Very often, ransomware attacks can be devastating to SMBs and can take down an organization in hours.

So being able to stop attackers before they get too far into your environment can save your company significant amounts of money and offer the opportunity to recover — something many unprepared businesses can't do after a ransomware attack.

Additionally, the ability to fix individual computers rather than shutting down entire systems means you may not have to stop all company operations in the case of a breach. This, too, limits the costs and damage associated with a breach.

Many EDR solutions also allow you to take actions remotely to hunt for, contain, and eradicate threats — all things that became critically important with the shift to working remotely.

Finally, many EDR solutions don't use signature-based detection, so they're leaner tools that take up less disk space and CPU utilization. Not only will you save computer utilization, but employees will appreciate that EDR tools won't slow down their machine in the same way antivirus software does



03.

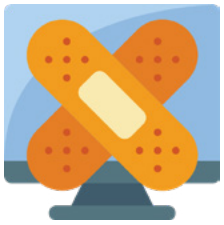
MAKE TIME TO REGULARLY PATCH SOFTWARE

One of the easiest ways to improve your security posture is to ask your IT team to patch software at least once a month. The time between when a patch is released and when the associated exploit is released is shrinking dramatically. Just last year, that time frame was 60 days. Now, a hacker will know how to exploit a patched vulnerability in only 43 days; making this yet another area where you need to act fast.

Prioritize patching

With so much on their plates already, IT teams may not have time to implement every patch that's released - prioritization will be incredibly helpful here. Any programs that are on the internet need to be patched immediately. The same goes for any endpoint software like email or web browsers. If an attacker can anonymously take action across the internet, it's a big threat to your organization.

Privilege escalation is important, but not as important as anything on the internet or cloud. And if it's not a remote code execution or denial of service attack, your teams don't need to overextend themselves trying to patch it on super short timelines.



Your security team or an outside security expert should review patches and set a priority list, identifying which patches need to be implemented within seven, 30, 60, and 90 days of release. By having a priority list that closely aligns with vulnerability, you'll save time and have fewer fire drills down the line.

04.

GET PROACTIVE WITH DECEPTION TACTICS

In addition to basic defenses, your security strategy should include deception tools and tactics that trick adversaries into revealing their location, intentions, and the tools and techniques they used to break into and persist in your environment. With detection tools, you can determine where someone is in the attack lifecycle and cut them off quickly. Proper deception requires a number of pieces working together to provide you with enough information to confidently detect and eliminate bad actors.

A quick-hit history of deception

Not too long ago, security professionals would drop honeypots throughout their networks and hope a hacker would just run into them. However, it became fairly easy for attackers to recognize and avoid honeypots, so a more advanced solution was needed.

Many companies use Active Directory to manage all the user accounts in their company. While this solution is easy to implement, it is very difficult to implement in a secure manner. Many hackers are experts at using Active Directory to quickly increase and expand their control across a company. As a result, some security folks started creating deceptive or canary accounts in Active Directory and watch closely for their use.

Though this strategy proved to be effective for some time, hackers started to pick up on clues to identify these deceptive objects. They noticed when fake items didn't align with the actual Active Directory objects, so this tactic failed as well. Some deception software companies have even published PowerShell scripts that can quickly query Active Directory and identify all of the fake or deceptive accounts. Right or wrong, this action exposed to the world what hackers were already doing to avoid deceptive objects.

The new wave of deception

Modern deception strategies call for the use of false Active Directory objects, breadcrumbs (artifacts that lead to honeypots), and honeypots. Ideally, you'd intercept hackers searching Active Directory, then return a poisoned response that leads to a honeypot or honey account. Rather than creating false objects, you should use items that actually exist in in your Active Directory. The same goes for admin accounts that hackers might try to exploit — lure attackers to real accounts that aren't real admins. The key is to present a real story that would convince attackers to continue down the path to the honeypot. It's even better if you can hide all real Active Directory objects and present only deceptive objects. Some products allow you to do this. If you have this capability, be sure to scrutinize your objects to make sure attackers can't identify them as deceptive.

This type of deception strategy takes thoughtful planning, and it might be difficult to create convincing stories if you're not an experienced penetration tester. You need to have a deep understanding of what hackers are looking for today and how they validate which objects are real. You then have to create objects and perhaps write small programs to continually refresh your objects.

Get creative with deception

To develop a truly effective deception strategy, you need to get into the minds of hackers and get creative with your tactics.

Attackers like to rummage through code repositories, ticketing systems, chat logs, and SharePoint, which means these are great places to set traps. If you have an internal red team, task them with exploring your network and identifying common mistakes your administrators make like oversharing or allowing too many permissions. Then replicate these errors with purely deceptive objects.

Add web beacons to documents so you can tell when obscure file locations are searched or viewed. Create a false passwords document, add a beacon to it, and upload it to your systems. Not only will you be alerted if someone reads the file, but you can track where the attacker is when they try one of these accounts. This is a great tactic because you will receive few false positive alerts. If someone is using a fake password, you know they're acting maliciously or curiously. Once you have the basics down, work with experts to contemplate how to leave breadcrumbs in public locations like LinkedIn, Github, and Reddit. Once you start thinking deceptively, the possibilities for creating a fake story are endless and intriguing.

Take an offensive stance

Deceptive strategies are the one time when the defender has an advantage over the attacker. Usually, companies are playing catch-up, chasing an attacker through their environment. But deception buys you time as you monitor how an attacker is moving through your systems and gives you an opportunity to come up with a strategy to stop them while they're busy in a false reality.

At one point, the consensus was to be very secret about using deception. But data now shows that when attackers know you have deception, they are more cautious and move more slowly through your environment, which is ultimately a win for you.

05.

GET 24/7 PROTECTION WITH A MANAGED DETECTION AND RESPONSE SERVICE

It's no longer enough to purchase and implement a series of cybersecurity tools. Cybersecurity requires humans to actively hunt for and respond to threats, and that work needs to be **happening 24/7**. Unfortunately, these managed detection and response (MDR) efforts can't be done by a single member of your IT or security teams.

The shortcomings of in-house MDR

First, it's important to note that while IT and security are both incredibly valuable to an organization, they are not the same. IT should not be tasked with your organization's security — nor will they want to be. Also, because security requires 24/7 coverage, a single hire won't be able to handle your entire security program. All security managers will want to sleep, take time off on the weekends, and occasionally step away to go on vacation. If they're solely responsible for your organization's security, you're left vulnerable any time they're not at their desk watching for threats.

This is especially important because many attacks are coming from outside the U.S. where time zones and holidays don't align with yours. Attackers know this.

That's why most ransomware attacks happen after hours or on weekends.

Organizations large and small need a deep bench of security experts working to protect their businesses. These experts need to understand malware, lateral movement, and how to hunt and respond to threats. Given that security is vital to an organization's survival and there is currently a shortage of skilled security professionals, these experts are in high demand. It's very difficult for businesses, especially small businesses, to attract and retain talent. Even entry-level security professionals are expensive hires, and many are chomping at the bit to work at large organizations where they have both more work and more support.

Outsource to an MSSP

To counter these trends, most companies choose to outsource their MDR efforts to an MDR service provider or MSSP. These vendors can accomplish the work at a fraction of the price of hiring an in-house security team — and they have the resources to do the job well.

When working with a good MDR or MSSP, you'll typically authorize them to not only monitor your environment and alert you when there's an issue, but to act on your behalf if an attacker is found.

Cybersecurity is a game where seconds count,

and if your MSSP waits for your approval before taking action, an attacker has already done too much damage. Competent security partners will be well on their way to solving the issue by the time you see an alert about it.

Because MSSPs are comprised of teams of security experts, 24/7 coverage isn't an issue. MSSPs are also working with a variety of clients, so they're abreast of the latest tools and techniques used by attackers and can monitor your environment for signs that they're being used against you — something an in-house team might not have time to research.

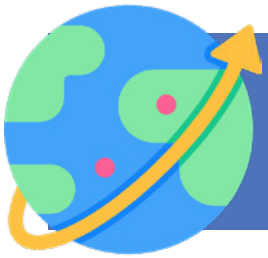
The modern MSSP

Not all security service providers are created equal, and some are more equipped to handle MDR than others. MDR used to be hyper-focused on networks, firewalls, and firewall logs. It was the first thing an MDR or MSSP would ask for when signing you on as a client. But technology has changed, and firewall logs aren't nearly as effective as endpoint detection and response technology. As covered in Chapter 2, this technology provides a much better view of incoming attacks and is much smarter than firewalls.

These days, MSSP may not even need your firewall logs, which saves you a ton of time and money. Firewalls are also loud because they create a lot of noise to work well. They can still be useful in the response stage but are rarely used in the detection phase. So if firewall logs are a big part of an MSSP's MDR strategy, it's probably not the MSSP for you.

Get the security that matters with SolCyber

SolCyber is a modern MSSP, offering amazing security managed by approachable humans at an incredible value. Our Foundational Coverage includes the security that matters and nothing more, so you can rest assured you're protected without overpaying.



Our services are designed to help small to mid-sized businesses gain the same coverage as Fortune 100 companies.

Learn more about the SolCyber difference and drop us a note to learn more about how we provide you with the security that matters.