CYBERSECURITY MADE SIMPLE

A GETTING STARTED GUIDE

Barkly™

JACK DANAHY
Co-founder and CTO, Barkly

Anthem, Experian, Target, JPMorgan Chase, Home Depot, Ebay. Big public breaches and the reporting around them can lead us to believe that it's only large companies that get hacked. Someone, or some organization, has specifically targeted them for their secrets, their users, or their financials.

As a result, smaller companies feel that they are relatively safe, simply because they have so much less to offer. While I was meeting with a technology group recently, one IT director summed it up: "We really don't have much that is very interesting, so why would anyone bother?"

Unfortunately, current statistics and the most successful attack techniques show that this conclusion is dangerously false. In fact, smaller companies have as much need to prioritize their own security as any other business of any size:

- In 2014, 60% of all targeted attacks struck small- and medium-sized organizations (Symantec).
- 1 in 2 businesses surveyed by the National Small Business Association in 2014 reported being victims of cyber attacks.
- 3 out of 4 spear-phishing attacks in August 2015 targeted small businesses with 250 employees or less.
- 60% of SMB cybercrime victims go out of business within 6 months of an attack (NCSA).

THE PURPOSE OF THIS GUIDE

This guide is designed to do three things:

1. **Educate you** on the latest cyber threats that exist for your company – specifically if you have a small- and medium-sized businesses – so you can know what you're up against.
2. **Empower you** to take appropriate precautions and start actively safeguarding not just your own cybersecurity, but the security of your customers.
3. **Enable you** to get started now. Security is a complex and rapidly evolving field. It's easy to get overwhelmed. Rather than try to boil the ocean, this guide will help you a) hone in on what your top security priorities are; and b) establish a solid foundation strategy that will serve you well no matter what solutions you buy or approaches you take.

WHO THIS GUIDE IS FOR?

Small business owners who know security should be a concern, but aren't sure where to start.

IT directors who only have so much time to devote to security.

Security managers who want to maximize their limited budget and resources.

PART I:

KNOW YOUR WEAKNESSES & YOUR STRENGTHS

Barkly™

THE TOP 5 CYBERSECURITY CHALLENGES TO OVERCOME

It's far too easy to fall into the trap of simply purchasing the latest technology and thinking all of your security problems will go away.

Lance Spitzner
Research and Community Director, SANS Securing the Human

Barkly

No. 1

Not Knowing There's a Problem: Security as a Blind Spot

The first (and arguably biggest) challenge businesses face is that they don't think cyber attacks will happen to them. This can be especially true for small businesses, who may assume they don't warrant much attention from attackers. According to a survey by Endurance International Group, over one third of small businesses do not have any cybersecurity measures in place, despite the fact that small- and medium-sized businesses bore the brunt of targeted attacks (60%) in 2014 (Symantec).

How do attackers have time to seek out so many individual small businesses? The answer is they don't, nor do they have to.

CRIMES OF OPPORTUNITY

There are any number of ways attackers can land and take advantage of malicious code on users' machines.

- Organizations as diverse as Forbes, Match.com, and Google have all been used as mules to carry advertising-enabled malware (malvertising) to their visitors and users.
- Legitimate websites get hacked, and malicious code is served up from them.
- Phishing campaigns attack lists of contacts simulating outreach from banks, retailers, or government agencies.

> If your customers can't trust you to be responsible with their information, they'll take their business elsewhere.

These attacks can be broadly directed and indiscriminately applied. The victims are not targeted because of where they work, they are just vulnerable places to land.

IT directors and security managers at smaller companies need to go to their management armed with facts to show them that their limited size and assets will not protect them from attacks (we'll cover specific tips to help you secure buy-in in Part II). These breaches begin with exploits that are blind to their targets, but the lack of security investment by small businesses can actually make them more attractive targets for additional attacks, as the attackers know they are far less likely to be discovered and disturbed.

If your customers can't trust you to be responsible with their information, they'll take their business elsewhere.

For all of these reasons, security at your small business has to be reevaluated. Companies of all sizes are exposed to a very similar set of dangers, and small businesses must abandon the false comfort of their relative obscurity and take control of the active protection of their data and their livelihoods.

No. 2

Not Knowing How to Break Down the Problem

With an ever-increasing number of cyberthreats and a bewildering array of security solutions available, the next challenge many companies face is determining where to even begin. Security is a complex issue. And like any complex issue, the best way to start addressing it is by breaking it down. Otherwise, the search for simple answers can easily lead to confusion and frustration, and it's common to find yourself pulled in multiple directions without knowing which one is really the right one for you.

BEFORE YOU CONSIDER SECURITY SOLUTIONS

"What product should I start with?" is a tempting first question to jump to, but if you don't have a basic understanding of what it is you're trying to solve, you're likely to end up buying a hammer only to realize later those weren't really nails you had, after all, they were screws.

Better questions to start with are:

- Why do we need better security?
- What are we trying to secure?
- What will happen if we don't get this right?

Security is a complex issue. And like any complex issue, the best way to start addressing it is by breaking it down.

The answers to those questions will provide you with the proper bearings and solid footing you need to head off in a productive direction. In Part II, we'll discuss in more detail how to use these three core questions to conduct a diagnostic self-evaluation.

No. 3

Not Having the Expertise to Address the Problem

Once you have a clear understanding of your problem and what it is you want to accomplish, naturally the next big question is, who's going to own all this?

For some small business owners and many IT pros, the immediate answer may be, "I am." Perhaps because you don't have a choice. According to Forbes, currently more than 200,000 U.S. cybersecurity jobs are unfilled, and the shortage is expected to reach 1.5 million unfilled positions by 2019. That shortage in security talent has sent demand soaring, and with the average salary rising to over $97,000, finding and hiring dedicated security professionals can be prohibitive for many organizations.

For those who are lucky enough to have options, however, here are three things to keep in mind:

- Hiring a security person (internal or external) won't inherently make your organization more secure.
- Not hiring a security person doesn't mean you don't have a security function. It just means you're it.
- Lack of in-house expertise has been cited as the top reason why companies regret investments in security technology (Ponemon's *2015 Global Study on IT Security Spending & Investments*). Buying a solution without having someone with the time and skills to manage it isn't a good investment.

According to Forbes, currently more than 200,000 U.S. cybersecurity jobs are unfilled, and the shortage is expected to reach 1.5 million unfilled positions by 2019.

Regardless of whether or not a dedicated security person is in the cards (see Part II for more tips on hiring and outsourcing), you will need to find ways to gather and/or leverage the expertise necessary to develop and implement a basic action plan. And even if you do have in-house or outsourced help, the more context and understanding you personally have, the better prepared you'll be to provide productive management and oversight.

No. 4

Not Having Resources Necessary to Carry Out an Action Plan

Most small business owners and IT pros are no strangers to stretching a budget. But security is particularly difficult. The majority of solutions are expensive, in many cases you may feel the need to invest in a variety to fit your needs. Sticker-shock aside, however, perhaps the biggest challenge security advocates face is that it's notoriously difficult to demonstrate ROI. With no direct correlation between money spent and improved security, it can be incredibly difficult to get leadership buy-in and approval.

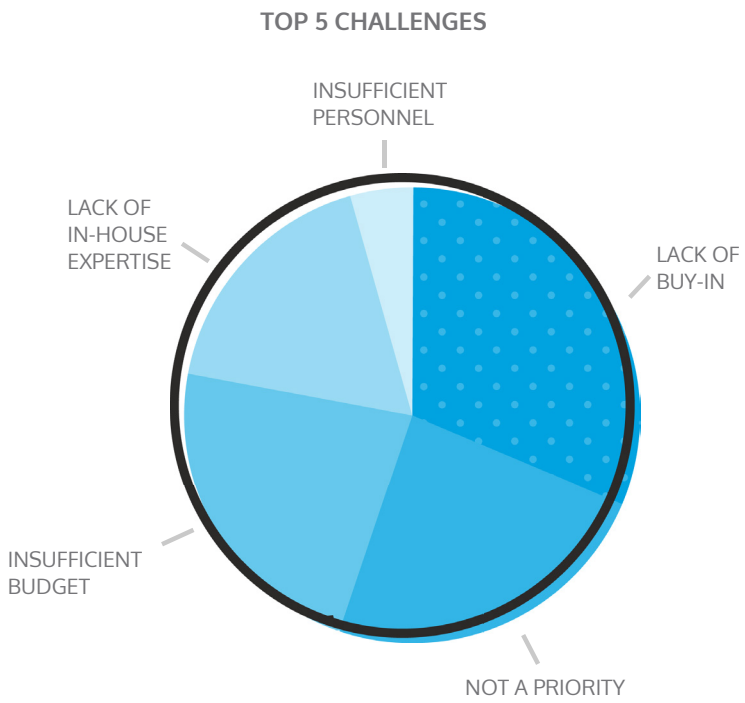
Nearly 60% of SMBs see buy-in as their #1 challenge that prevents a fully effective IT security posture (Ponemon).

There are several things that should happen before you approach leadership with a shopping list to sign off on. If your first conversation regarding security is around budget, you're doing it wrong. Rather than clearing line items, your focus should be on reaching an agreement on what's important for your business, first.

Once you've defined those priorities, you can then go about setting the bar for security at your organization and determining what it will take for you to reach it. That way, when you come across any budgeting issues, you can couch the discussion in terms of what everyone agreed is important.

We'll share more tips on how to set the bar with your leadership team in Part II.

Nearly 60% of SMBs see buy-in as their #1 challenge that prevents a fully effective IT security posture.



No. 5

Your Arch Nemesis: Inertia

When it comes to security, the only wrong answer is doing nothing.

For all the security challenges your business faces, the biggest threat isn't a sophisticated piece of malware, it's ambivalence and complacency. Nothing strips the efficacy from existing security initiatives faster, and nothing makes it more difficult to adopt anything new. Nothing makes companies more vulnerable. Nothing is more important or challenging to overcome.

It can be easy to think of security as a technical problem, but the truth is any meaningful solution requires not just the adoption of new software and techniques, but new mindsets and habits, too. In order to overcome the crippling inertia that's holding back many of your peers, you'll have to take on two negative attitudes that are particularly pervasive.

When it comes to security, the only wrong answer is doing nothing.

TWO ATTITUDES TO FIGHT

1. **Security isn't important:** As long as this attitude exists in your organization you've got an uphill battle on your hands. Until you're able to break through to executives and employees by connecting it to their other priorities and goals, sadly, security is going to be one of those things they don't fully appreciate until it's gone. The key is to start building a shared sense of ownership, buy-in, and responsibility before you get to that point.
2. **Complete security isn't possible, so why bother:** While technically true, too often the "no silver bullet" mentality can result in companies lowering their expectations. Yes, every company should prepare for the worst, but that shouldn't stop them from demanding more from vendors and striving to accomplish more, themselves.

   Companies can't afford business as usual. Cost per cyber attack has more than doubled in just two years, rising from $8,699 in 2012 to $20,752 in 2014. With limited resources and security expertise at their disposal, small businesses in particular are becoming big targets, but the good news is you don't have to take things lying down. In the next section, we'll cover five ways you can turn what you may see as weaknesses into surprisingly powerful strengths.

UNLEASHING YOUR HIDDEN STRENGTHS

If you have a big castle, it's hard to defend, but if you have a smaller castle, it's easier.

Heather Adkins
Information Security Manager, Google

Barkly

Simple is Easier to Secure than Complex

The good news is that, once aware of your top challenges, you may actually have a simpler time getting secure than larger companies with 10x or even 100x your budget. Those big businesses may have considerable resources at their disposal, but that doesn't necessarily mean they can deploy them quickly or efficiently.

Don't rush to add complexity to your security. It's better to embrace your role as David than try to slip into a lumbering Goliath's shoes.

As the list below indicates, "big security" isn't always better security. Being part of a smaller organization can provide you with certain natural advantages you should embrace. By leveraging them effectively, not only will security feel more manageable, you'll also be able to accomplish more with less.

1) A SMALLER ATTACK SURFACE IS EASIER TO DEFEND

Think of your attack surface as all the different points that potentially expose your system to an attack. These can include open ports, web applications with potential vulnerabilities, users with access credentials, etc. The more complexity you introduce (the more users and types of users you add, for example), the larger the attack surface becomes.

By their nature, small businesses generally start out with a smaller attack surface. That's an advantage they should try to hold onto as long as they can as they grow, taking steps to actively map, manage, and reduce their attack surface whenever possible. For more tips on how to do that, see OWASP's *Attack Surface Analysis Cheat Sheet*.

Don't rush to add complexity to your security. It's better to embrace your role as David than try to slip into a lumbering Goliath's shoes.

2) A SMALLER SYSTEM IS EASIER TO MONITOR

Having fewer machines also means you can watch them more closely without flooding a management system. Even the best security teams at large companies can get overwhelmed sorting through onslaughts of data. Having greater visibility and less noise to filter is a big advantage.

As you grow, you'll want to investigate automation and continue to find ways to limit the information you have to process.

3) A FRESH START CAN BE EVEN BETTER THAN A HEAD START

When you're rolling out a new security initiative, starting out with a blank canvas can actually be a blessing in disguise. Larger companies often have a hefty amount of legacy baggage to deal with. Existing policies and solutions can pose significant hurdles to innovation, especially when they're budget sponges or compatibility nightmares.

That's also something to keep in mind during any purchase and policy decisions you make as your company grows. We'll look into how the top five security technologies can integrate and enable each other in Part III.

Simple is Easier to Secure than Complex

4) A FLAT ORGANIZATION IS EASIER TO TRANSFORM

Because smaller organizations tend to be flatter and more centralized, it's easier to develop a true culture of security where everyone feels a sense of ownership and responsibility. Security policies and initiatives can also be better tailored to suit the specific needs of departments and individuals, allowing them to be more relevant and less general.

5) FEWER EMPLOYEES ARE EASIER TO MANAGE

When 77% of small business IT pros say employees are the single weakest link in their security infrastructure (CloudEntr) it's easy to understand why having fewer of them can be an advantage. In addition to reducing your attack surface, it can also give you more opportunity for group as well as one-on-one training. That is key, because inspiring all of your employees to participate in the security of the company is what will ultimately pay the highest dividend.

For tips on training your employees effectively, see our eBook, *The Realist's Guide to Cybersecurity Awareness*.

BOTTOM LINE

Security can often seem complicated, but as the list above demonstrates, there's power in simplicity. The more you can leverage these strengths in the early days of your security program, the better. As you grow, you'll need to regularly revisit and adjust your approaches. That is why it's so important to lay a solid foundation for your security now, so when it comes time to scale you can do so successfully, without things spiraling out of control.

PART I RECAP

- **Small doesn't mean safe, but it can mean quick and nimble.** In 2014, 60% of attacks were targeted toward SMBs. But while they typically have fewer resources to utilize against threats they also have natural advantages they can leverage.
- **Before you consider security solutions you need to understand your specific needs.** Otherwise you can end up with a hammer when your problem wasn't really a nail.
- **Security isn't just one person's responsibility.** That said, you do need someone with expertise actively owning and managing it. Spending money on solutions is a waste if no one knows how to leverage them properly.
- **The biggest threat you face is complacency.** Improving security can require significant change, and change requires buy-in. The most important thing you can do is convince leadership that security is important and worth investing in.
- **There's power in simplicity.** "Big security" isn't always better security. Try to keep things simple and streamlined as long as you can.

PART II:

LAYING THE FOUNDATION

Barkly™

SETTING THE BAR FOR YOUR SECURITY

If you don't have a sense of the goal posts you are kicking toward, I can almost guarantee you will miss.

Ryan Berg
Chief Scientist, Barkly

Barkly

"MORE" IS NOT A STRATEGY

With high-profile data breaches continuing to make headlines with disturbing regularity, the general consensus on the cybersecurity front is that we need to be doing more. Of course, the $100 billion dollar question is, doing more of what?

Unless you and your leadership team are fond of throwing money at problems indiscriminately, the following isn't exactly a strategy you should take or expect to get approved:

1. Get a bigger budget.
2. ???
3. Improved security.

According to Gartner, global spending on IT security is set to cross the $100 billion mark in 2018.

A more realistic list of steps might look something like this:

1. Determine your needs.
2. Agree on what's important.
3. Determine what it will take to accomplish that.
4. Execute against your plan.
5. Review, iterate, and repeat.

To help you get started let's dive deeper into each step.

Step 1

Determine Your Needs

Setting the bar for your security program starts with stepping back and performing a diagnostic self-evaluation. That may sound complicated, but don't worry, it's not. A good approach is to ask three simple core questions:

- Why do we need better security?
- What are we trying to secure?
- What will happen if we don't get this right?

Let's take a deeper dive into what you can surface from each.

1) WHY DO WE NEED BETTER SECURITY?
A common approach when you're just starting out with security is to look at what other companies are doing and use that as a basis for your own decision making. While that can be helpful, you'll always better served ironing out your own unique problems and needs first. Otherwise, you can find yourself drawn to a seemingly popular solution that addresses others' problems, but not your own.

By asking this question, you can develop sharper clarity around your organization's motivations for improving security in the first place. Have you suffered a data breach? Are you worried about employees falling for phishing scams? Is your priority to prevent downtime or to protect personal customer information?

From there, try to understand the specific reasons your organization isn't secure enough and develop focused goals around what you want to accomplish. The point is to hone in on the kinds of solutions that are going to help not just anyone, but you, specifically.

2) WHAT ARE WE TRYING TO SECURE?
For many, the gut reaction to this question is "my networks," but when pressed or when given more time to think, others might answer, "my data," "my business," "my reputation," or "my time."

Depending on your goal, your answer can then lead to a litany of other questions that will help you build an inventory of the resources you need to protect and develop even more clarity around your specific needs.

- What are your critical assets?
- What is your current state of coverage for those assets?
- What are your gaps?

Answering these questions will help you move away from the ineffective task of vaguely trying to protect everything from everything to a general degree.

Determine Your Needs

Remember, it is impossible to make an informed decision about any security solution or approach until you know what it is you are supposed to secure and how secure it has to be.

3) WHAT WILL HAPPEN IF WE DON'T GET THIS RIGHT?
This is another crucial question to ask at the start of any new security program. That's because knowing whether what you're setting out to do is imperative or just interesting will make all the difference when it comes time to make tough but necessary choices.

If failure will mean the loss of jobs, revenue, and reputation, you can likely expect robust executive support for purchasing and implementing solutions, even if doing so means disrupting the status quo.

If, on the other hand, failure has less significant consequences, that may inform your decision to either push hard or compromise when you're facing the chilly realities of funding, inconvenience, and change.

Step 2

Agree On What's Important

Now that you have a basic understanding of where you'd like to start, it's time to get the other key stakeholders in your organization involved. The sooner they become part of the conversation, the better, because nothing sets a security initiative up for utter failure like a lack of comprehensive buy-in.

Your goal during this step is to accomplish two things:

1. Come to a universal agreement on why security is a necessary investment for your organization in the first place.
2. Get everyone on the same page regarding priorities, challenges, and goals.

Depending on how savvy and informed your leadership team is around cybersecurity, your first task may be to provide information and stats to bring them up to speed and underscore its importance.

> The key to a productive "buy-in" conversation is not to focus on how the business can improve security, but how security can improve the business.

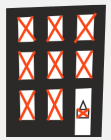
Small businesses in particular may be operating under the false assumption that they're safe from cyber attacks. If that's the case for your company, here are some stats to set the record straight:

In 2014, **60% of all targeted attacks** struck small- and medium-sized organizations. (Symantec)

1 in 2 businesses surveyed by the National Small Business Association in 2014 reported being victims of cyber attacks.

3 out of 4 spear-phishing attacks in August 2015 targeted small businesses with 250 employees or less. (Symantec)

The average cost-per-attack has skyrocketed to $20,752 (National Small Business Association).



60% of SMB cybercrime victims go out of business within 6 months of an attack. (NCSA)

Agree On What's Important

Walk through the same three core questions you answered in step 1, but in addition to identifying what the security priorities are, this time try to develop a clear understanding of how those priorities relate back to your organization's primary business goals.

The key to a productive "buy-in" conversation is not to focus on how the business can improve security, but how security can improve the business.

Remember, your leadership team doesn't have to understand how security works, but they do need to understand why you're doing what you're doing, and be on board with what you're ultimately trying to achieve.

Having this type of honest discussion up front isn't always easy, but it's well worth it in the long run. Not only will it help you establish a clear sense of what's important for the business, it will also allow you to move forward with the confidence knowing your leadership team is fully on board with your agreed upon objectives.

Step 3

Determine What It Will Take to Accomplish Your Goals

ESTABLISHING THE BASIS FOR YOUR BUDGET

Budget discussions around cybersecurity are rarely easy, in part because it's so notoriously difficult to measure and demonstrate ROI. Many compare it with investing in insurance – increasing your spending doesn't inherently make you safer, it simply reduces your risk and helps you prepare for if and when things go wrong.

That means unless you're actively dealing with a hack or a breach, security spending often isn't the easiest thing to get people excited about. Too often, it's either an afterthought or it's money that gets assigned once everyone else has already grabbed their piece of the pie.

You need to establish that security is a budgetary item that needs dedicated dollars assigned to it. It shouldn't be money that's coming from another place or that can be reassigned if marketing needs to do a new advertising campaign.

In an ideal world, once you've set your bar with your leadership team, a budget discussion should flow naturally. As long as you have a universal agreement that your goals are important to the business, then you should be able to come back to leadership with a list of things you need to execute in order to hit those goals. The wrinkle, of course, is knowing what kinds of investments are actually going to deliver.

What technologies and services are truly necessary? Is data backup more important than active network monitoring? Do you need a $10,000 firewall or will a $2,000 firewall do the trick?

Again, this is where your answers to the three core questions will come in handy, but an additional approach for companies not sure where to begin is to look at the *Building Security in Maturity Model* (BSIMM) from Cigital. While it won't provide specific answers for determining what's right for you, it does offer a glimpse into what other companies of various sizes and growth stages in your industry are doing, which is good context to have.

> Don't waste your money and political capital trying to keep up with the Joneses. Spending isn't what makes you secure.

WARNING: WHAT NOT TO DO

Be careful not to base your security planning and budgeting entirely on what others are doing. Just because a competitor has a security information and event management (SIEM) solution doesn't mean you need to have one, and just because you spend 15% of your total IT budget on security and they only spend 10% doesn't mean you're inherently more secure.

Determine What It Will Take to Accomplish Your Goals

Don't waste your money and political capital trying to keep up with the Joneses. Spending isn't what makes you secure.

There's a big difference between using competitor research and industry benchmarks to inform your decisions and allowing those things to make your decisions for you.

The point isn't to find a killer game plan to steal. You'll still need to develop a custom blueprint that addresses your own unique needs. But by getting a sense of what constitutes good, better, and best practices for other companies you may have an easier job determining where you're strong, where you're weak, where it's okay for you to be weak, and where you need to invest.

THE BEST WAY TO HANDLE BUDGET DISAGREEMENTS

There's bound to be push and pull when it comes to spending, and there may be times when you're told the money you need simply isn't there. But when that happens you need to bring the conversation back to the shared priorities you established with the leadership team. You should be able to say, "Remember the things we agreed were important? These are the activities and investments we've identified in order to hit our bar."

You can still disagree on specific requirements, and you may have to make concessions or get creative to cut down on costs, but as long as you have that common ground to fall back on you should be able to have an intelligent discussion around the tradeoffs between coverage and risk.

ADDITIONAL RESOURCES

Budgeting for Information Security (Entrepreneur)

Roundtable: Advice on IT Security Budget Management (TechTarget)

OUTSOURCING VS. IN-HOUSE

One question many companies grapple with, especially in the early days of their initiatives, is deciding whether or not to outsource at least some aspect of their security to managed security service providers (MSSPs).

There are many cases when outsourcing can make sense:

- You may not have the appropriate skills and resources available in-house.
- You may not be in a position to make a full-time hire, let alone multiple hires.
- You may not be able to find the right person to fill a full-time role (according to Forbes, we're in the midst of a cybersecurity workforce shortage expected to reach 1.5 million unfilled positions by 2019).

For all of those reasons, we're seeing a boom in the managed security services market, which is expected to grow from $8 billion in 2015 to $30 billion by 2020.

Determine What It Will Take to Accomplish Your Goals

So is getting outside help the answer for you? Possibly. But before you even think about outsourcing, you need to develop your own clear idea of what it is you're actually looking for help with in the first place.

YOU'RE NOT READY FOR OUTSOURCING IF...

- You're not able to clearly articulate your problem or goal.
- You don't know where your assets are or what it is you're trying to secure.
- You don't have someone on board to actively own and manage the relationship.

Companies need to be very careful not to give outsourcers the impression that they don't know what they need. The reality is many of them will see dollar signs and may guide you to toward the solutions that are easiest for them to implement, but aren't actually the solutions that best fit your needs.

Think of it this way: If you go to a brake shop because you think you've got a brake problem, you're more than likely going to find yourself coughing up the cash for new brakes. Meanwhile, you may actually have a bigger issue wrong with the car that's still going unaddressed. Your shiny new brakes may work like a charm, but you can still get into an accident if your steering is off, and if you go back to the brake shop angry they're just going to shrug and say of course they didn't protect you for that.

The best approach to outsourcing requires thought and planning in advance. The worst thing you can say to a managed security service provider is, "I don't know where to start."

OUTSOURCING ONLY WORKS WHEN...

- You have a clearly-defined problem to solve or goal to achieve.
- You find a vendor you can work well with and trust to deliver on your specific needs.

There's no lack of outsourced security options to choose from. But if you determine you have a specific goal that lends itself particularly well to being delegated outside your company, you can then begin to whittle down the list to providers that specialize in that area.

On the next page, let's review ten things you should be sure to discuss with any outsourcer before you sign an agreement.

Determine What It Will Take to Accomplish Your Goals

10 THINGS TO CONSIDER TO EVALUATE MANAGED SECURITY SERVICE PROVIDERS (MSSPS)

1. Find out whether they've worked with comparable companies that are similar in size, stage, and/or industry.
2. Get references!
3. Review their standards, policies, and procedures carefully.
4. Make sure all requirements and responsibilities will be documented in service level agreements and/or statements of work.
5. Determine who on their side will be owning your account and what your level of interaction will be (you don't want to go into a partnership expecting access to the Principal only to find out later that's not the case).
6. Have clear milestones and deliveries to checkpoint progress against the SLA along the way.
7. Understand what type of access to internal resources will be necessary and make sure you have everything available before they show up the first day.
8. Understand any reseller agreements they have in place.
9. Get a clear understanding of their financials. The last thing you need is a company in poor financial position willing to say yes to everything simply because they need the work.
10. Have an exit strategy for if/when you want to stop using their services.

ONE LAST NOTE OF CAUTION ON OUTSOURCING

Remember, no one outside your business is going to value your business as much as you do. When you outsource aspects of your company's security you are putting your safety and success in their hands. You may pay for a level of professionalism, but when it comes down to it, an MSSP will act with his/her best interests in mind.

You ultimately own the security of your organization, if a security incident happens it will be your name in the news not your outsourced provider. That is why it is extremely important you understand what problems you are trying to solve before you start writing a check.

Outsourcing isn't something you should jump into too quickly. To succeed, it requires a considerable amount of planning, discussion, and building trust.

Step 4

Execute Against Your Plan

Once you've come to an agreement around what's important for you to accomplish and determined what you think it will take to do so, the next step is to develop your roadmap and get to it!

If you still need help ironing out a basic plan of attack, go back to the questions and answers you developed in response to the "What are we trying to secure?" prompt in Step 1. Here are a few more you may find helpful:

- What are your critical assets?
- What is your current state of coverage for those assets?
- What level of coverage/risk are you willing to accept?
- What are your gaps?
- What can you do to close those gaps?
- How will you measure success?

Do you need to hire a dedicated security manager to accomplish your goals? Not necessarily, but someone will need to fill the security management role.

WHO OWNS EXECUTION?

As we covered in Part I and with our tips regarding outsourcing, determining who will actively manage security is just as important as determining what exactly that management entails. Do you need to hire a dedicated security manager to accomplish your goals? Not necessarily, but keep in mind someone will need to fill the security management role. Just how much security expertise that person needs will depend on your specific needs, goals, and solutions.

Don't lose sight of the fact that better security requires four things:

1. People
2. Process
3. Technology
4. An organizational commitment to all three

Step 5

Review, Iterate, and Repeat

Without a regular review process it's remarkable how quickly a new security initiative can lose momentum and effectiveness. It's far too easy for a fresh approach to become the stale status quo, and in the rapidly evolving world of security, stale is seldom secure.

The key is to establish a regular cadence of going back to your plan, reexamining your priorities and goals, reviewing your results, and discussing what changes or adjustments need to be made to keep everything aligned. Otherwise, you run the risk of discovering too late your budget and efforts haven't actually been flowing to the right needs.

A recent study from the Ponemon Institute reveals how common this problem is. As the stats below show, many companies suffer from a damaging misalignment between where their money is being funneled and what's actually perceived to be the most effective and necessary solutions:

- 84% of companies are investing in intrusion detection or prevention systems, yet only 41% believe they are a top-performing solution.
- On the other hand, 63% of respondents listed security incident and event management systems (SIEM) as a top-performing technology, but only 53% are actively investing in it.
- Despite negligent insiders being one of the top reported concerns, only 8% of companies listed cybersecurity training as a top objective.

AVOIDING THE "MORE MONEY, SAME PROBLEMS" PATTERN WITH REGULAR REVIEWS

Security cannot be approached as a one-and-done activity. As nice as it is to imagine you can simply check off a series of boxes and move on, that's unfortunately not how it works. Every day, new attacks are discovered and new vulnerabilities exposed. To keep up, you need to adopt an incremental and iterative approach that provides you with regular opportunities to learn, adjust, and improve.

- Determine the right cadence for reviewing your progress.
- Reaffirm your top priorities and goals.
- Ensure your time, effort, and budget is indeed flowing to the right needs.
- See that any new or changing priorities are reflected in your plan.

Again, as long as you're able to achieve and maintain clarity around your top needs and priorities, you can ensure you're building your security on a solid foundation.

PART II RECAP

- **"More" is not a strategy.** Before you spend a dime on security you need to develop both clarity and buy-in around your top priorities and goals.
- **Leadership cares about the business, not security.** The key to a productive "buy-in" conversation is not to focus on how the business can improve security, but how security can improve the business.
- **Spending isn't what makes you secure.** Don't waste your money and political capital trying to keep up with the Joneses.
- **Outsourcing can make sense.** But only if you have a clearly-defined goal to achieve or problem to solve.
- **You may not need a dedicated security manager.** But you will need someone to fill the security management role.
- **Improving security isn't a one-and-done activity.** It requires an ongoing, active, and iterative approach.

PART III:
SUITING UP

Barkly™

SIZING UP POTENTIAL SOLUTIONS

Barkly

Sizing Up Potential Solutions

If you've made it this far, this should go without saying. But just in case you skipped ahead:

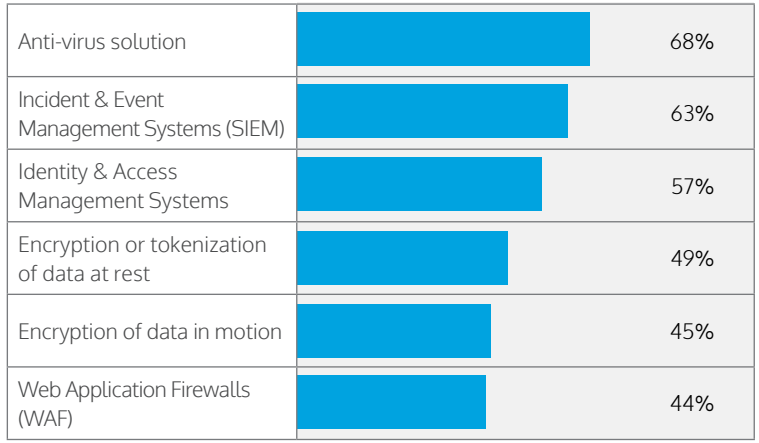
You shouldn't spend a dime on a new security solution without understanding your own specific needs and priorities first.

With that out of the way, let's look at a simple exercise that should help you arrive at more informed – and ultimately more successful – purchasing decisions.

Even if you're feeling the heat from management and auditors to improve security now, don't be rushed into making a purchasing decision without first understanding how to:

1. Maximize the value you are getting from your existing, underused solutions.
2. Identify the most likely areas where a little new investment or effort will make a big difference.

To help illustrate an example of how you can better evaluate solutions, let's look at the top security technologies as ranked by IT security practitioners in a recent survey conducted by the Ponemon Institute:



2015 Global Study on IT Security Spending & Investments, Ponemon Institute

Now let's take a closer look at these protection technologies and walk through their potential positive impact on your organization, how effective they actually tend to be in practice, their relative cost, and some simple pros and cons.

Sizing Up Potential Solutions

TECHNOLOGY	PURPOSE	COST	BENEFIT	LIMITING FACTORS
Anti-Virus (A/V)	Keep dangerous software off my systems.	$	Easy to use, good on known viruses, and can be operated with little security experience.	Provides limited protection due to reliance on signatures of known attacks. Frequently criticized for slowing down user systems.
Security Information & Event Management (SIEM)	Identify unauthorized or destructive behavior across my network.	$$$	Provides a broad view of security across an enterprise, and stronger breach detection capability across multiple systems.	SIEM tooling is costly to purchase and more costly to staff. The volume of data and complexity of the information provided requires experienced analysts and there are multiple examples of attacks going undetected in this flood of information.
Identity & Access Management (IAM)	Enable only authorized access to systems and services, and tie individuals to those accesses.	$$$	Strong access protection and audit, and the cornerstone of knowing who touched what and when. Good single sign-on can simplify user experience.	Dynamic organizations and increasing numbers of applications and services make it difficult to maintain IAM integration across new apps and among the changing roles of users. IAM also requires logging, as user authenticating information is under threat from credential theft attacks and keystroke loggers.
Encryption	Keep my data obscured from everyone who lacks the authority to see it.	$	Keeps information obscured from unauthorized viewers at rest and in transit.	Encryption is only as strong as the user authenticating information and the integrity of the systems on which it runs. When either the user information or user system is compromised, encryption is effectively disabled on that system.
Firewalls	Create a gateway to separate internal networks from external traffic, and to block threatening network actions.	$$	Good baseline security to create a logical perimeter for monitoring and access control. A good information source on attempted inbound attacks and outbound data theft.	Firewall logs become noisier as traffic flows increase, and increasing encrypted traffic flows can impede the firewall's ability to see attacks inbound. Firewalls are also less useful against custom-crafted and browser-based attacks which deliver attack content in a fragmented means or through the use of a dropper or downloader. Firewalls also cannot protect mobile or remote user systems when they are used outside the firewalled network.

Remember that these are all simply tools. Used successfully, they can provide protection and be integrated to improve each other's effectiveness. Used incorrectly or disjointedly, they can create the illusion of security and leave the unknowing organization in an even worse state.

Sizing Up Potential Solutions

Here are some recommendations on maximizing the combined value from tools you may already have in-house by understanding how they can support each other. We've prioritized them by the increased value that the integration can bring.

	BASE					
ENABLER		Anti-Virus (A/V)	Security Information & Event Management (SIEM)	Identity & Access Management (IAM)	Encryption	Firewalls
	Anti-Virus (A/V)		⚡⚡⚡	⚡	⚡	
	Security Information & Event Management (SIEM)	⚡		⚡		⚡⚡
	Identity & Access Management (IAM)		⚡⚡⚡		⚡	⚡
	Encryption		⚡⚡⚡	⚡		
	Firewalls	⚡⚡	⚡⚡	⚡	⚡	

⚡⚡⚡ High integration boost ⚡⚡ Medium integration boost ⚡ Modest integration boost

Sizing Up Potential Solutions

A/V AS AN ENABLING TECHNOLOGY

Endpoint protection is a critical factor in the efficacy of almost every other security technology.

As a result, there is a clear benefit to improving A/V, change management, and endpoint protection as you look for ways to improve your defenses at low cost.

SIEM AS AN ENABLING TECHNOLOGY

Security information and event management (SIEM) can be thought of as a "bird's-eye" view of an organization's security. The major benefit of SIEM to other security technologies is to improve their coverage and understand their gaps.

When attacks are discovered, most SIEMs allow their data to be used to automatically limit inbound access through the creation of firewall rules. SIEMs can also be used to identify unexpected traffic or request from infected systems, which can be used to identify systems in need of system or A/V update.

IAM AS AN ENABLING TECHNOLOGY

Identity and access management (IAM) is the foundation of understanding the appropriateness and authorization of behavior on the network. For example, a SIEM is most useful when if can be used to associated expected behaviors with individual users, and to identify offending user accounts when it encounters malicious behavior.

IAM also provides a more granular means of integrating firewall-based perimeter access control, and of auditing the inbound and outbound traffic from users. Without IAM, or with weak IAM, non-repudiable attributions are either difficult or impossible.

ENCRYPTION AS AN ENABLING TECHNOLOGY

Encryption is the center of authentication, secure transmission, and secure storage of data. As such, encryption is closely associated with the ways in which users validate their identity to the IAM. Encryption also provides protected channels through which confidential or high-integrity data will be fed to the SIEM. Firewalls also gain additional value when used as a point of terminus for encrypted connections and VPN's from trusted external sources.

Without encryption, much of this internetworking and monitoring would become untrustable.

FIREWALLS AS AN ENABLER

While the perimeter of a network is becoming increasingly amorphous, firewalls offer increased efficiency for local security, like anti-virus, by doing some of the heavy lifting. By stripping attachment file types, and doing A/V scanning at the gateway, they can reduce the load on user devices.

Similarly, by limiting traffic flows, they can also decrease the glut of traffic monitored by the SIEM. Firewalls keep external connections from forging internal access credentials and can be configured to increase privacy by only allowing encrypted traffic to leave the network to certain destinations.

PART IV:

MALWARE MANUAL

KNOWING WHAT YOU'RE UP AGAINST

Barkly

KNOWING WHAT YOU'RE UP AGAINST

The more you understand what you're up against, the better you can prepare your defense. In this section, you'll learn the characteristics of six classes of malware – what makes them dangerous and what they were created to accomplish at your expense. But first, let's take a closer look at the different elements involved in any cyber attack.

ELEMENTS OF A CYBER ATTACK

- **Endpoint**: The target of the attack. The purpose of the attack is to control, corrupt, or disable the endpoint.
- **Vulnerability**: The weakness that permits the endpoint to be penetrated. Vulnerabilities include software flaws, system design weaknesses, insecure configurations, and even human errors.
- **Malware**: Malicious software. There are many different types of malware, and attacks often involve more than one. As you'll see in the following pages, one way to classify them is by their purpose or intended effect.
- **The delivery vehicle**: Malware is delivered to victim machines through a variety of techniques from social engineering (phishing, etc.) to USB sticks.
- **Method of execution (MoE)**: The means through which attackers get the resources necessary (access, processing time, data, etc.) to execute an attack.

In order for security protection to successfully stop a cyber attack it needs to thwart malware from achieving its purpose or desired effect.

MALWARE CLASS

Depositors

Malware whose primary purpose is to land and expand

WHY THEY WERE CREATED

To conceal the introduction of malware by separating the exploit of the system from the execution and installation of the malicious program.

TWO BASIC TYPES

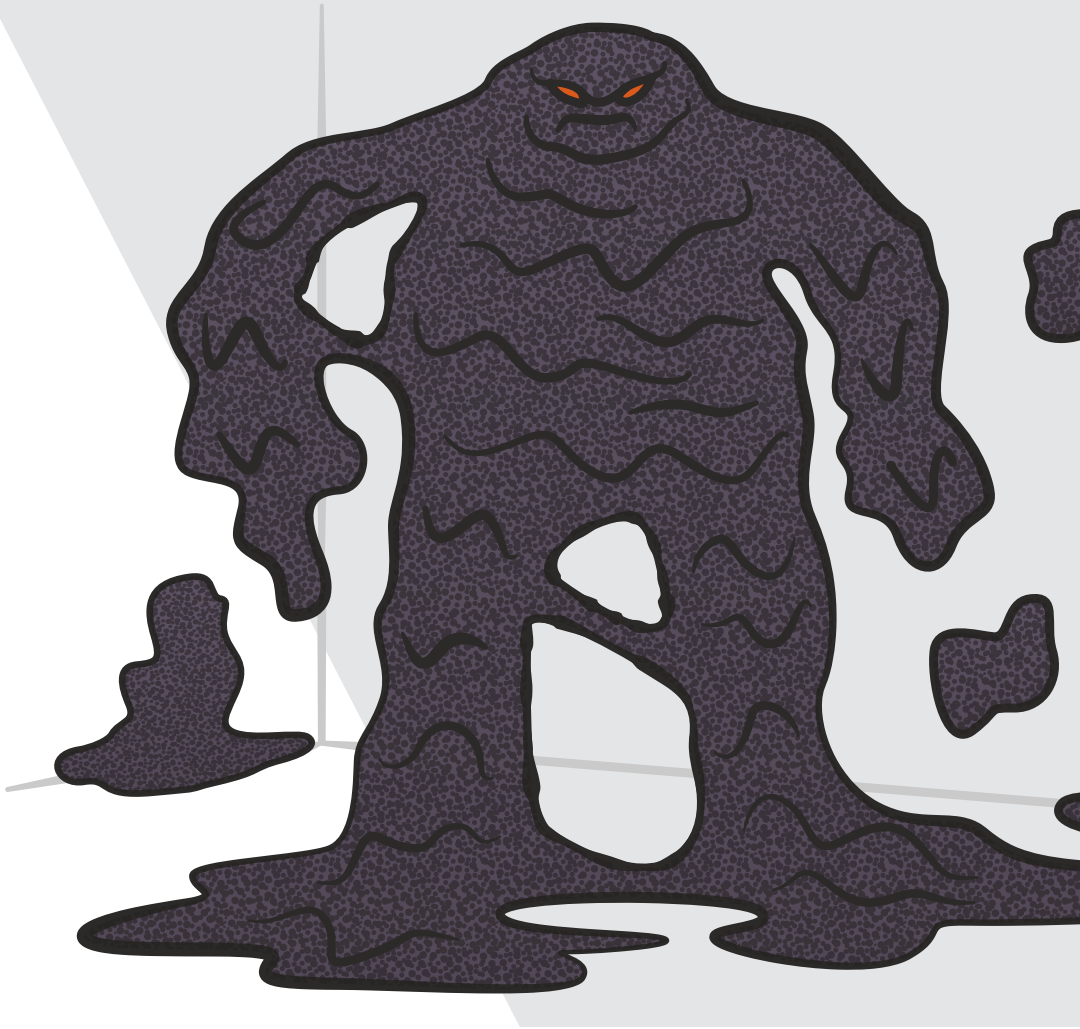
- **Downloader**: A type of trojan program that, once running, fetches and installs the malware executables.
- **Dropper**: A type of trojan executable that combines both the installation functionality and the actual malware program within the same object. As a result, a dropper does not necessarily require a permissive network connection.

WHY THEY'RE DANGEROUS

Depositors allow attackers to sneak malware past traditional security before transforming it into its executable form.

EXAMPLE IN ACTION

Cryptowall 2.0 utilized a sophisticated dropper that embedded multiple potential exploits to infiltrate target systems. It performed anti-VM and anti-emulation checks prior to decrypting and executing the malware, decreasing the likelihood of identification and detection, and had the capability of executing 64-bit code from a 32-bit dropper.



MALWARE CLASS

Ransomware

Malware that threatens to destroy data unless a victim makes payment

WHY THEY WERE CREATED

To extort money from victims.

TWO BASIC TYPES

- **Encrypting Ransomware**: Takes an inventory of system files, and then encrypts either all or part of the critical assets. Victims are shown a screen with instructions on how to pay an untraceable ransom to decrypt the files.
- **Destructive Ransomware**: Demonstrates its presence on the system, disabling administrator access, and demands payment to avoid the automatic destruction of data or system operation.

WHY THEY'RE DANGEROUS

Ransomware provides attackers with an easy and lucrative way to monetize their exploits on systems. Inexpensive and extensible ransomware packages are common and freely available. Like depositors, ransomware can lie dormant for long periods of time, avoiding detection and making it difficult to trace.

EXAMPLE IN ACTION

The most notorious examples of ransomware are Cryptowall and Cryptolocker, which have reportedly cost over $48 million in payments.

MALWARE CLASS

Backdoors

Malware that provides at-will unauthorized remote access or command and control

WHY THEY WERE CREATED

To give attackers repeated and unfettered access to exploited systems for reconnaissance, or to leverage systems for botnets or future attacks against others.

WHAT THEY DO

Backdoors find ways to make their existence persistent and undetected across reboots, providing attackers the ability to tap back into the system and reconnect. Botnets are the most common type of backdoor.

WHY THEY'RE DANGEROUS

Any good attack will take the time to leave a machine open to future visits via a backdoor, and they spread rapidly. In 2014, it was reported that 18 systems were infected with botnets every second.

MALWARE CLASS

Credential Stealers

Malware used to steal user IDs, passwords, or session authorization

WHY THEY WERE CREATED

For most attackers, getting onto one machine is just a start. Once there, they want to see and steal the IDs and passwords that give access to a much larger number of systems, services, and accounts.

WHAT THEY DO

Credential stealers can operate in any number of ways. The easiest way is to install a keystroke logger that will record every key that is struck, showing all your IDs and passwords. For other systems, they can wait until you establish an authorized connection and steal the active credential information of the session in which you're operating.

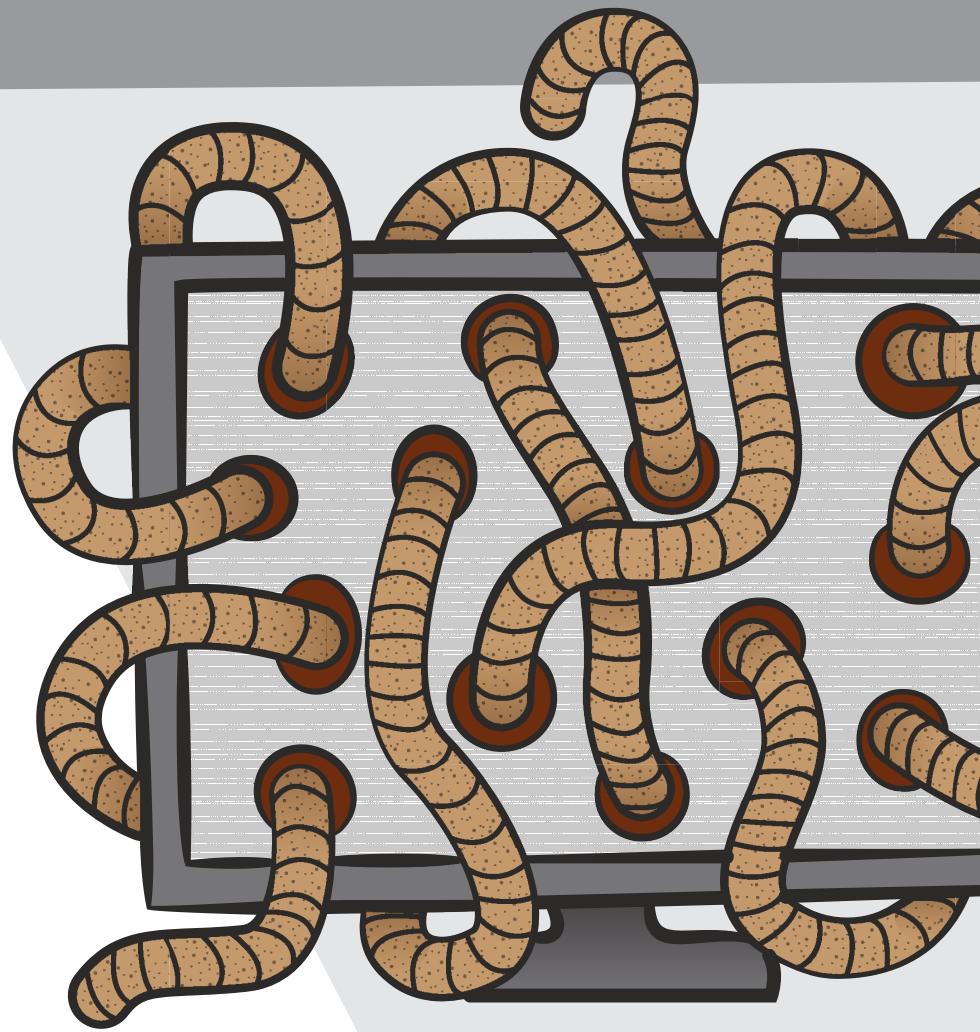
WHY THEY'RE DANGEROUS

By leveraging just one user's system, attackers can gain access to a host of local machines, hosted services, and critical servers, which, in addition to providing assets to steal, will be used to expand the attacker's reach.

MALWARE CLASS

Virus / Worm

Self-replicating, self-perpetuating malware



WHY THEY WERE CREATED

Viruses and worms infect host systems and then spread to infect others autonomously.

WHAT THEY DO

Once on a system, viruses and worms insert copies of themselves into programs, files, and drives. Worms can then execute actions to spread onto other computers via their network. Worms and viruses can also carry additional "payloads" designed to perform harmful or disruptive activity on their infected hosts.

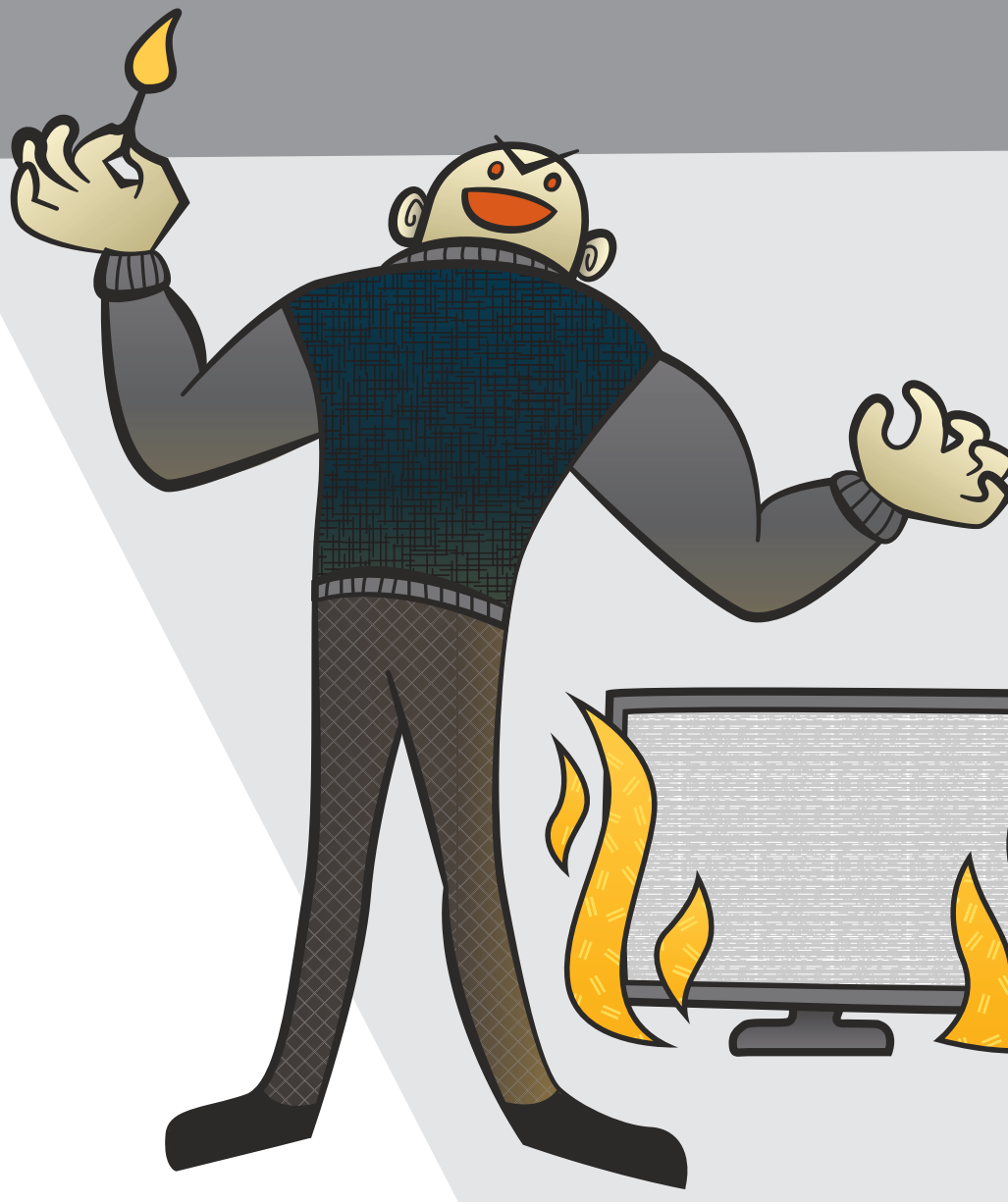
WHY THEY'RE DANGEROUS

This class of malware creates damage that rapidly becomes widespread. Worms can enable attackers to create a network of hijacked machines (a botnet) for use as spam hubs or distributed denial-of-service (DDoS) attack centers, while viruses are often shared by unaware users who go on to infect others.

MALWARE CLASS

Vandalizers

Malware that is purely destructive in nature



WHY THEY WERE CREATED

To damage and/or deface websites, systems, and machines.

WHAT THEY DO

Once a vandalizer has access to a vulnerable site it can replace site content, redirect users to other locations, or bring the system down completely.

WHY THEY'RE DANGEROUS

Vandalizer attacks can strike without warning and be very public. Unlike ransomware, they don't give victims the opportunity to pay up to avoid the attack. A successful vandalizer can make systems inoperable, permanently destroy data and configurations, and create protracted downtime.

EXAMPLE IN ACTION

The Syrian Electronic Army has prominently used vandalizers to hit such high-profile media companies as the Associated Press, the New York Times, and the Washington Post. In the latter case, visitors to the Post's mobile site received pop-up alerts with propaganda messages.

WARNING: MALWARE CAN AND ALMOST ALWAYS DOES TEAM UP

It's important to recognize these classes of malware rarely operate in isolation. Good cyber attacks will involve multiple classes of malware to increase effectiveness, enable rapid propagation, or obfuscate underlying operations.

As an example, attackers could use a downloader to establish a command and control infrastructure for ransomware, then they might use a worm to propagate a vandalizer against monitoring systems, and steal credentials to a hosted email account to spread the ransomware further.

CONCLUSION: KEY TAKEAWAYS & NEXT STEPS

Barkly™

Data breaches. Ransomware. State-of-the-art attacks targeting big corporations and small businesses alike. Rarely a day goes by without a stark reminder in the headlines that improving security should be a high priority. For many of us, however, that remains an abstract and unapproachable goal.

With this eBook, we set out to help you change that by a) clearing up the misconception that you need to be an expert to understand security basics; and b) providing you with a simple framework that encourages and enables you to get started now.

To recap, on the right is a checklist of the key steps covered in this guide. Once completed, you will have armed yourself with a core security strategy, security process, and leadership buy-in – the cornerstone pieces of a good defense.

Have questions around these or any other cybersecurity-related topics?
Find the answers on our blog.

CHECKLIST: 10 THINGS TO DO TO GET YOUR SECURITY PROGRAM OFF THE GROUND

- ☐ Leadership understands cybersecurity is an important need that requires a dedicated budget.
  For convincing stats to help you make the case, see our infographic, "Small Business Cybersecurity: It's Time to Fight Back."
- ☐ I have answers to the three core questions:

  Why do we need better security?
  What are we trying to secure?
  What will happen if we don't get this right?

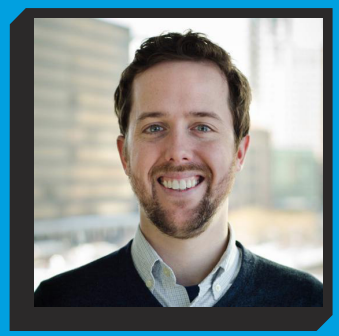
  If you're having trouble with these, go back to Part II, Step 1 for help.
- ☐ We have defined – and leadership is bought in on – our priorities, challenges, and goals for security.
- ☐ There is a clear in-house owner for security initiatives.
- ☐ I've developed a security roadmap by determining the following:

  I have a prioritized inventory of assets we need to protect.
  I know the current state of coverage for those assets.
  I've assessed the gaps in current coverage and desired coverage.
- ☐ I've determined what solutions I need to close those gaps.
  Don't know where to start? See Part III for help.
- ☐ I've determined what expertise I need in-house and/or via outsourcing to implement those solutions effectively.
- ☐ I've developed a budget accordingly.
- ☐ I've established a regular cadence for reviewing progress and reaffirming priorities and goals.
- ☐ I've developed a simple cybersecurity awareness program for training employees on basics.
  To get started see our eBook The Realist's Guide to Cybersecurity Awareness.

We want your feedback!

Now that you've read the guide let us know what you think! Please take a second to answer three short questions that can help us create more interesting and useful content.

GIVE YOUR FEEDBACK



Jonathan Crowe
Senior Content Manager, Barkly

At Barkly, we believe security shouldn't have to be difficult to use or understand. That's why we're building a simple solution designed to safeguard your company with strong endpoint protection that's fast, affordable, and easy-to-use.

Share the Cybersecurity Made Simple guide on Twitter

SHARE

STAY INFORMED! SUBSCRIBE TO THE BARKLY BLOG:
blog.barkly.com