How to secure your software faster and better

Real-world strategy for fixing security vulnerabilities, building secure software and winning sales

Ted Harrington, leader of ethical hackers and Infosec Skills author

INFOSEC™

Introduction

Hey, I'm Ted Harrington, #1 best-selling author of Hackable. I've helped hundreds of companies fix tens of thousands of security vulnerabilities, including Google, Amazon and Netflix. I love teaching cybersecurity leaders like you how to improve your application security, whether that's through my courses on Infosec Skills, my book or this ebook collection of articles. I've packed years of experience into the three sections of this ebook — common challenges, approaches to those challenges and security success. You'll learn how to avoid mistakes, where to invest your money and how to gain the competitive edge. Got questions? Connect with me on LinkedIn and book a meeting at Infosec to learn more about team training!

Who is Ted Harrington?

Infosec Instructor Ted Harrington is the best-selling author of "HACKABLE: How to Do Application Security Right," and the Executive Partner at Independent Security Evaluators (ISE), the company of ethical hackers famous for hacking cars, medical devices, web applications and password managers. Ted has been featured in more than 100 media outlets, including The Wall Street Journal, Financial Times and Forbes. His team founded and organizes IoT Village, an event whose hacking contest is a three-time DEF CON Black Badge winner. He hosts the Tech Done Different podcast.

What's in this ebook?

Challenges: What you're up against

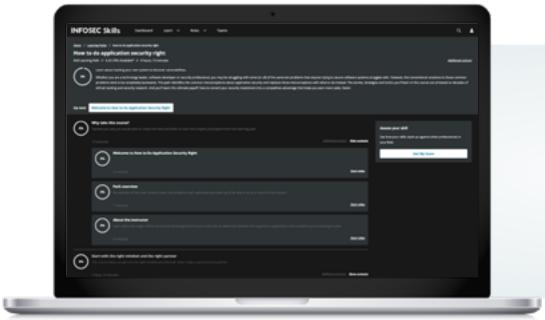
Approach: What's the best way to secure software?

Success: Getting it right, repeatedly

Learn how to do application security right

Whether you are a technology leader, software developer or security professional, you may be struggling with some (or all) of the same problems that anyone trying to secure software systems struggles with. However, the conventional solutions to those common problems tend to be completely backwards.

That's why I created an 11-course Infosec Skills learning path How to Do Application Security Right. This path identifies the common misconceptions about application security and replaces those misconceptions with what to do instead. The stories, strategies and tactics you'll learn in these courses are all based on decades of ethical hacking and security research.


INFOSEC Skills
How to do application security right
Why take this course?
Welcome to How to Do Application Security Right
Path overview
About the instructor
Start with the right mindset and the right partner
Assess your skill

Create your free Infosec Skills account to browse my courses — or click here to talk to someone about advancing your career.

More from Infosec and Ted Harrington

Learn how to do application security right

Watch my Infosec Edge webcast on "How to Do Application Security Right"

Watch Now

Read my articles on Infosec Resources

See Articles

Get a copy of my book "How to Do Application Security Right"

Buy Now

Check out my Cyber Work Podcast episode

Watch Now

Challenges

WHAT YOU'RE UP AGAINST

"The question is not whether vulnerabilities exist in your application — they do. The real question is simply which happens first: will attackers exploit them, or will you fix them?"

— Ted Harrington

Why a skills shortage is one of the biggest security challenges for companies

5 problems with securing applications

3 major flaws of the black-box approach to security testing

Why a skills shortage is one of the biggest security challenges for companies

Almost every company building an application needs to secure it, and yet all of them face an enormous constraint: talent.

Security requires a highly specialized skill set, which is in extreme shortage and will continue to be so for the foreseeable future. There are several reasons for this skills shortage, ranging from limitations in formal education to misperceptions about what a career in security even entails.

Your company can't have adequate security without skilled individuals making it happen, so what can you do to build the right security team?

By understanding the talent shortage, you can anticipate what to do about it.

Education is a security bottleneck

The first cause behind the security-talent shortage is education and experience opportunities. Formal education isn't (yet) optimized to create enough security talent.

Many ethical hackers come out of computer science degree programs, yet most programs treat security as an area of interest, rather than a core discipline. Security-specific degree programs are popping up, but there still aren't enough of

Want to learn more about overcoming the skills shortage? Check out my course "Start with the right mindset and the right partner."

Get Started

We'll help you meet your cybersecurity training goals: Book meeting

them to produce enough skilled security professionals, let alone at the level of expertise that's needed.

Furthermore, security requires extensive, real-world experience outside of the classroom, too. Most security degree programs teach the fundamentals, but what security professionals do in the field usually differs from what they learn in the classroom.

Developing security skills takes a long time and requires accumulating deep expertise across a broad range of domains. There's no single place where all of this information can be found, so it takes a lot of grit just to find the relevant information, let alone master it. Taken together, these factors mean that formal education produces fewer qualified security professionals than the world needs.

Security has perception issues

The second cause behind the talent shortage is a common perception that security is ridiculously hard. Rising computer scientists (of which ethical hackers are a subset) often pursue other things instead.

This misunderstanding of the field also feeds into a perception that, as one ethical hacker put it, "Security people are seen as wizards beyond mortal understanding." This suggests that if you're not already one of them, it's not worth trying to become one.

That simply isn't true: the best security professionals — literally every single one of them — learned the skills along the way, too. Nevertheless, this perception deters a lot of talented people from even getting started.

Security is adversarial

Lastly, security by its very nature is adversarial. The purpose is to pit two forces against each other. It's not just about being creative (as is the case with almost all of computer science); it's about being more creative than someone else. To succeed in the security field, you need to outsmart the hackers working against you, a requirement that can be stressful and intimidating.

We'll help you meet your cybersecurity training goals: Book meeting

To succeed in the security field, you need to outsmart the hackers working against you, a requirement that can be stressful and intimidating.

Many talented people decide they'd rather compete against the constraints of what it takes to develop software than compete against other people. Most computer scientists want to build things for themselves, rather than tear apart the work of others. Yet, that's exactly what ethical hacking is about.

Like the perception issues around the difficulty of security, the adversarial nature of the career keeps many qualified people from ever starting.

Dealing with the shortage

As a company that needs skilled security professionals, what are you to do in the face of this shortage?

Your best option is to take a two-pronged approach: build your own expertise in-house, and also hire an external security team. Security is a team sport, and you should pursue both. External and internal expertise complement each other and magnify each other's impact.

Your external security partner finds security vulnerabilities; you fix them. Your partner transfers knowledge; you use it to get better. Your external partner is immune to bias as well as the strong opinions of powerful leaders in your company; they just tell you how it is, even if it's not what you want to hear. You ensure the security mission is supported by executives and key stakeholders, while providing your partner with the access and information they need to improve your systems most efficiently.

The talent shortage might mean building your in-house team will be a long and difficult process. With an external team complementing your internal teams, you're able to deal with your many security challenges right away, while leaning on your external teams to help you build internal capabilities over time.

Win-win.

We'll help you meet your cybersecurity training goals: Book meeting

5 problems with securing applications

The question is not whether vulnerabilities exist in your application — they do. The real question is simply which happens first: will attackers exploit them, or will you fix them?

However, doing that can sometimes be easier said than done. For many companies, getting started on securing their application is riddled with logistical and practical challenges.

#1: Developers juggle many priorities

The first problem you might encounter relates to your developers' priorities. Your developers juggle many priorities, and security is just one. Yet, usually, the top levels of leadership determine which priorities to emphasize. Nevertheless, developers are expected to keep things secure, even if it's not made a top priority for them. That's a lot to deal with!

When leadership doesn't understand or prioritize security, your developers simply can't allocate sufficient time to it. As a leader, it's up to you to make sure your developers are empowered to prioritize security and devote a sufficient amount of time to its implementation. Otherwise, they won't have enough bandwidth to protect your applications.

The best way to deal with this is to ensure that the top levels of leadership at the company understand the core principles of security. A good way to do that is to make sure that the right type of security testing is being done in order to give the appropriate information to leaders so they can make good decisions.

Not sure how to triage vulnerabilities or what to address first? Find out in my course "Fix your vulnerabilities" where you'll discover two types of remediations and the three-phase process of implementing them.

Get Started

We'll help you meet your cybersecurity training goals: Book meeting

#2: Security usually isn't a developer's specialty

Your developers might understand the importance of security, but for most developers, security isn't the primary focus of their training.

Developers are usually brilliant people trying to build clean, efficient, effective code. However, they're not always thinking about how to break it. By contrast, attackers spend every waking minute studying how to break that clean, efficient, effective code.

The best way to deal with this is to hire security specialists internally or externally (or ideally, both) to lead your security effort in partnership with your developers.

#3: Deadline pressure causes security to be postponed

Another problem companies often face is the clash between security and deadlines. Companies tend to believe that security slows down development, while at the same time there's tremendous pressure to hit release dates. Security is often seen as something that causes delays in hitting release milestones and overall makes lives harder for developers. It's often also seen as something that can be deferred to later.

As a result, security tends to get postponed. However, this just causes regressions and rework later. It makes things harder and more expensive in the long run.

It's a lot easier than most people realize to build security into the development process. For every development action, there is a security action too. Take it. You already have the right people in the right room, having the right conversations, just expand those conversations to include security as well. The more involved aspects (such as security testing) are done by your security partner anyways, so they don't drag on your own engineering resources.

We'll help you meet your cybersecurity training goals: [Book meeting]

> **I've been in the trenches with many people battling these same challenges: misplaced priorities, capabilities limitations, shortage of talent, deadlines and relentless change. I understand why you might think security is a headache, but in reality, security is your best friend.**

#4: Security talent is scarce

Another problem you might face is the scarcity of security talent. There simply aren't enough skilled security professionals to meet the extreme demand for them.

Why the shortage? Security requires a highly specialized skill set, and formal education is not yet optimized to train enough workers with the necessary skills. Most programs treat security as an area of interest, rather than a core discipline. Also, security requires extensive, real-world experience that cannot be found in the classroom.

To deal with this problem, partner with an external security consulting firm while you gradually grow your in-house team. Eventually, you want to have both in-house and external security expertise, and by partnering first, you can overcome the talent shortage simply by hiring an external firm.

#5: Security is never done

Lastly, many companies treat security like a short-term annoyance to deal with before getting back to other things. However, the truth is that security is never done — it's an ongoing process and an investment in your company.

Change is the only constant. As technology shifts, so too does the security model. Software development itself is changing.

To succeed with your security efforts, acknowledge that security is a permanent part of your operating processes and expenses. Treat (and fund) it like an investment to maximize, rather than a tax to minimize. Deal with change through regular security assessments of your software system. The right cadence for most companies is every 3-6 months (rather than the every 1-2 years that most people do).

Overcome security challenges

As a leader of ethical hackers, I've been in the trenches with many people battling these same challenges: misplaced priorities, capabilities limitations, shortage of talent, deadlines and relentless change. I understand why you might think security is a headache, but in reality, security is your best friend.

We'll help you meet your cybersecurity training goals: Book meeting

Investing in security is not just the right thing to do; it also delivers a competitive advantage for your business. Proving that you're secure in the face of unknown threats is exactly how you earn the trust of your customers. That leads to more sales, more customers and more market share. It's how you become a leader in your field.

Security requires time, attention and money to do right, but if you can overcome the inherent problems that most people face, you'll build better, more secure software systems and obtain a competitive advantage.

We'll help you meet your cybersecurity training goals: Book meeting

3 major flaws of the black-box approach to security testing

Imagine a castle with a king who wants to know if he could be assassinated. He orders a loyal noble to send some knights to try to break into the castle. He gives no information to those knights about the castle defenses. After all, the king thinks that what he needs is for them to pretend to be his enemies, and his enemies don't have any of that information.

This is the black-box approach to security testing, the methodology that people frequently request. Unfortunately, they're usually unaware of its many drawbacks. In black-box, you don't tell your security evaluators anything about how the system works. The goal of the methodology is to limit information in an attempt to replicate real-world conditions, but it is flawed.

A few weeks later, the king is murdered. His enemies found a secret tunnel that the knights didn't know about and used it to get to the king. The king knew about this secret tunnel; it was his escape route in the event of a siege. But he never told the knights about it. By intentionally limiting information, the king lost his life.

Yes, this metaphor is a bit whimsical, but it makes clear why a black-box approach can be counterproductive. By understanding the methodology's three primary flaws, you and your security team can be more effective in protecting your company's assets.

Black-box flaw #1: You waste time and money

In our example, the knights spent time figuring out how deep the moat was, how many alligators were in it, and where it would be easiest to cross. But the king already knew all of these things, which means every minute the knights spent trying to figure them out didn't help the king.

By limiting the information supplied to your assessor, it requires them to invest resources — your time and your money — in obtaining information you could supply in minutes.

We'll help you meet your cybersecurity training goals: Book meeting

In this way, black-box security is inefficient. By limiting the information supplied to your assessor, it requires them to invest resources — your time and your money — in obtaining information you could supply in minutes. You literally pay them to figure out the things you already know. Worse yet, it rarely results in the same level of knowledge that would be delivered if you just told them.

The black-box approach risks your security assessor *only* providing you information you already know while missing the subtle vulnerabilities that you actually need them to identify.

Black-box flaw #2: You don't test your system; you test your partner

The king determined that these particular knights didn't break in within the amount of time they were allowed, but that didn't mean that other knights — let alone his enemies — couldn't. What had he actually evaluated? The knights, not his defenses.

The sneakiest drawback to black-box testing is that you aren't testing the system; you're testing your security partner. You determine whether *this* security expert can compromise *this* system within *this* amount of effort. That's pretty much it.

Instead, you want to vet the skills of your security partner before you start testing; it should not be the purpose of your testing. If you need to validate the skills of your assessors, there are better and less expensive ways to do that. Security is about finding and fixing flaws. However, black-box methodology is about limiting information, which limits value.

Want to learn more about black-box and other methods for your company? Check out my course "Choose the right assessment methodology."

Get Started

We'll help you meet your cybersecurity training goals: Book meeting

Black-box flaw #3: You get low-value results

Finally, black-box testing provides low-value results.

If vulnerabilities aren't found, it does not mean they don't exist; it simply means that the testing didn't find them yet. You have no way of knowing if there are other issues or even how close to discovering an issue they may have been. Security is about understanding and minimizing risk. A black-box methodology isn't well suited to deliver that.

Also, with black-box testing, you don't get helpful remediations. Your partners don't know how the system works, so they can't recommend how to fix any issues they find. You might be able to figure out the solution on your own. However, it puts the onus back on you to do the problem-solving. As a result, you lose the many years of experience that your security partner has with solving problems just like yours.

Ultimately, you get less value out of what you're paying for than if you fully informed your security partner going into testing.

An informed security partner is more effective

Imagine instead that the king walks the knights around the castle, pointing out the features of the walls, moats and turrets. As a result, the knights intimately understand the castle defenses and can probe accordingly for weaknesses. They'll find more vulnerabilities without wasting time and effort on things the king already knows. Better yet, because they understand how all the defenses work together, they'll be able to advise the king on how to fix any issues they find.

In the same way, informing your security partner about how your system works ensures that you'll avoid the flaws of black-box testing: wasted resources; testing the partner, not the system and low-value results.

Instead of black-box, get white-box. White-box is about sharing information. Sharing information maximizes the

We'll help you meet your cybersecurity training goals: Book meeting

value you get as a result. White-box testing is faster, more efficient and delivers more valuable results.

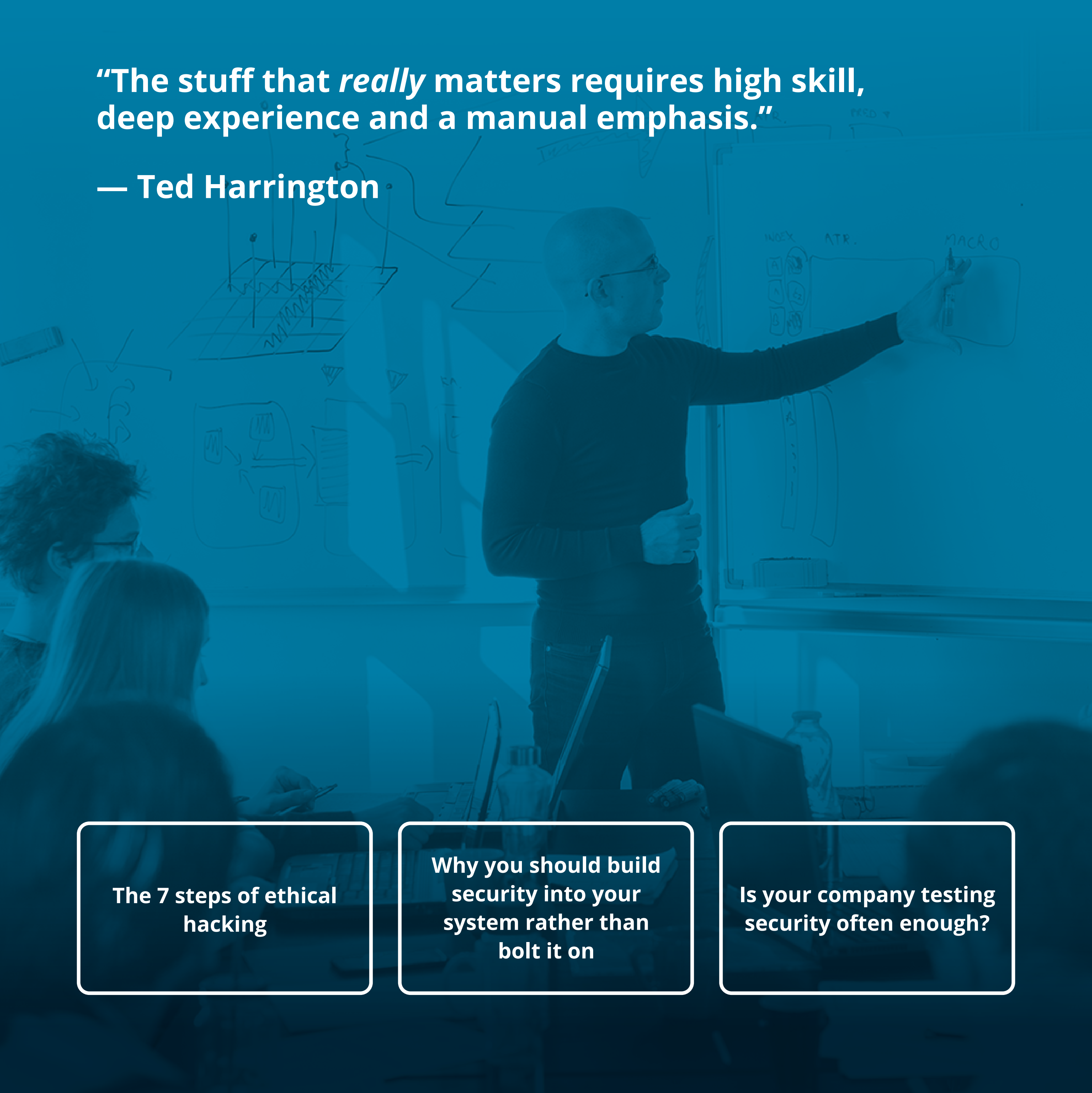
Good security is about collaboration, and collaboration delivers much more value than withholding information ever can. By understanding your system, your partner can help you secure it to the best of their ability.

We'll help you meet your cybersecurity training goals: Book meeting

Approach

WHAT'S THE BEST WAY TO SECURE SOFTWARE?

> "The stuff that *really* matters requires high skill, deep experience and a manual emphasis."
>
> — Ted Harrington



The 7 steps of ethical hacking

Why you should build security into your system rather than bolt it on

Is your company testing security often enough?

The 7 steps of ethical hacking

To beat hackers at their own game, you need to think like them. They're going to probe your software systems to find security vulnerabilities; you need to do this too.

But ... how?

If you're like most people, you struggle to understand how attackers think, how they operate and how they break systems. Worst of all, you may struggle to know what to do about it.

Believe it or not, there's a method to the madness, and I'm going to show you exactly what it is.

Step one: Hire an external security partner

Your first step is to hire an external security partner to do the hacking. You might think "*we can handle this in-house*," but your ethical hackers offer several unique benefits.

You want complete independence. An external expert provides an unbiased view; they'll tell you exactly how it is, even if it isn't what you want to hear. They didn't build your code, so they have no attachment to it.

By hiring an external partner, you capitalize on subject matter expertise that you probably don't have in-house. You get both the breadth and depth that come with a diverse team of experts, which most companies don't staff in-house. And you get all of that when you need it, and don't pay for it when you don't. Most companies don't need a full time team of ethical hackers in-house, so this is a cost efficient way to get expertise within the financial constraints of your business.

Beware, however, that not all partners are the same. Specializations and levels of skill vary widely, so make sure to vet potential security partners in order to hire the specialization and skills you need (if you struggle with this part, chapter 1 of "Hackable" explains in-depth how to do this).

We'll help you meet your cybersecurity training goals: Book meeting

Attackers want to abuse your system's functionality. That means you need to have your partner look for this too. By finding these vulnerabilities first, you can fix them and prevent abuse.

Step two: Analyze the design

To understand how to break the system, your partner needs to understand how it's supposed to work. That's why the next step is to analyze the design.

Your security partner should learn the fundamentals of the software: the features, how users navigate through it, how access is provisioned and where users can input values. They need to understand why it exists, what business problems it solves and what it protects.

They'll also want to evaluate for design flaws, which are vulnerabilities inherent in the system's design. Give your partner time to analyze for these flaws before moving on.

Unfortunately, many security approaches overlook this step. For example, if your partner is just running an automated scanner and that's all, it won't matter how the system works or why it works that way. Yet, the most important vulnerabilities tend to be impacted heavily by those factors.

Step three: Run scans

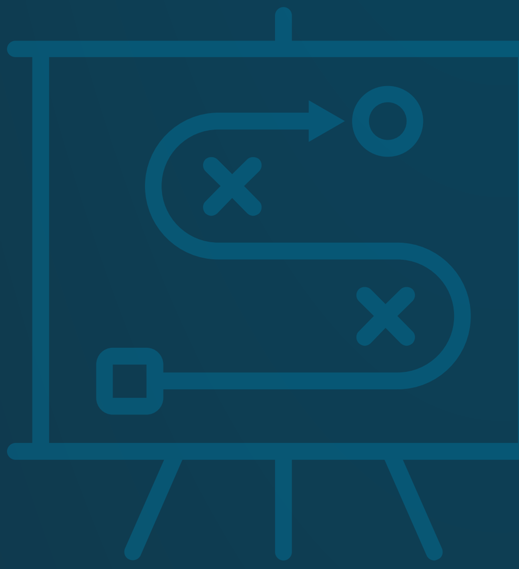
Next, your security partner should run scans, which are an efficient and inexpensive way to gain information that helps in later assessment stages. Scans quickly reveal the obvious issues that would require enormous effort to do manually. Most attackers run scans first, so it's a good idea for you to do this, too. You want to see what they'll see.

Keep in mind that scanning is not a comprehensive effort to find your security vulnerabilities; it's just one piece of the overall puzzle. However, many security approaches try to do exactly that. Reject that.

Step four: Look for known vulnerabilities

Attackers want the best results for the effort they invest, so the logical place to start is by looking where most people make mistakes. They seek these out as a shortcut to their success. Many software systems suffer the same mistakes, and so attackers explore the likely assumption that yours did too.

We'll help you meet your cybersecurity training goals: Book meeting



To defend successfully, your testing must check for common issues, including things like Injection Attacks, Broken Authentication and Broken Access Control. This is just a sampling of the ever-evolving types of issues your attackers know to look for. Your security partner should, too.

Caution: There's a capability gap

Unfortunately, most security testing calls it quits at this point. Many approaches don't even hit all of the steps mentioned so far: they rely solely on scans and fail to analyze the design.

The testing discussed so far requires minimal to moderate skill and experience and can be performed with a heavy emphasis on automated tools. But what comes next — the stuff that *really* matters — requires high skill, deep experience and a manual emphasis.

When you vet your partner — and then later agree on scope and methodology — make absolutely sure you're going to be getting everything that comes next. If you won't, choose a different partner.

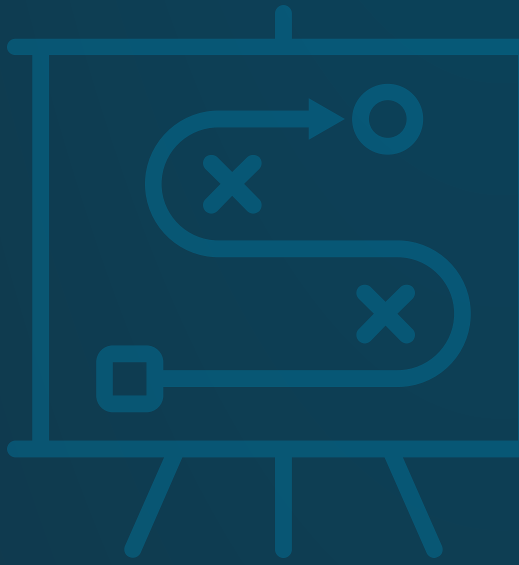
Your security partner should go beyond the fundamentals previously discussed and into the advanced tactics we're about to get into.

Step five: Abuse the system's functionality

Now that you've made sure to cross the capability gap, the next thing your security partner does is abuse the system's functionality. This uses an application's own features in an attack.

An example might be abusing the way a system treats integers: if the system is expecting positive integers, but negative integers are used instead, what happens? Or alternatively, can one user manipulate the password reset functionality to reset passwords for *other* users, thereby taking over their account?

Attackers want to abuse your system's functionality. That means you need to have your partner look for this too.



We'll help you meet your cybersecurity training goals: Book meeting

By finding these vulnerabilities first, you can fix them and prevent abuse.

There's no tool for this. You can't automate it. You must do it manually.

Step six: Chain exploits

The next step is exploit chaining, which is combining two or more vulnerabilities in order to multiply impact. Like timing jumps on a trampoline with a friend to send each other rocketing to new heights, chaining exploits enables attackers to cause even more damage.

In isolation, a couple of vulnerabilities might not be bad. In combination, they might be catastrophic. Vulnerabilities must be considered in the context of each other, rather than in isolation. Attackers seek to chain exploits, and you should, too. There's no tool for this. You can't automate it. You must do it manually.

Step seven: Seek the "unknown unknowns"

Lastly, your security partner will want to seek out "unknown unknowns," which are flaws so unexpected you don't even consider them.

This comes in numerous forms, including novel versions of common vulnerabilities and previously unknown attack methods. Dealing with unknown unknowns is the absolute pinnacle of security testing. It entails the most important issues you'll face.

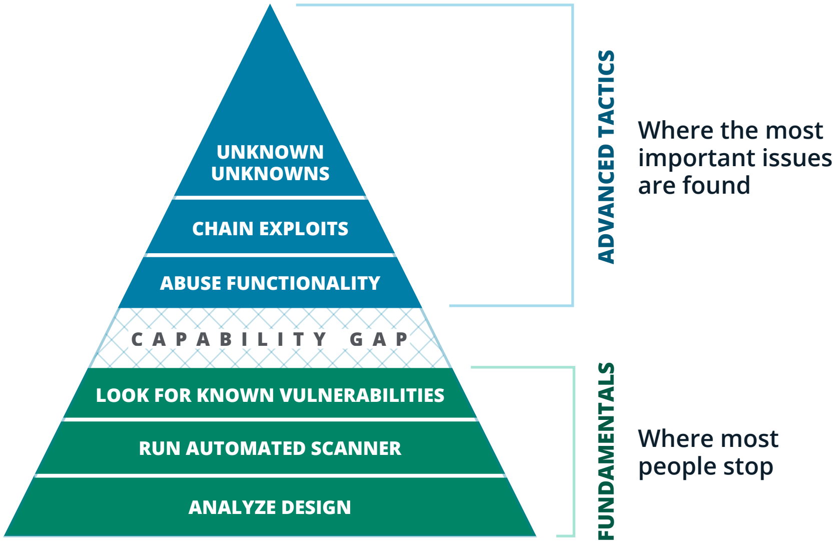
Want to dive deeper into chain exploits and learn more methods for uncovering system vulnerabilities? Check out my course "Hack your system."

Get Started

We'll help you meet your cybersecurity training goals: Book meeting

To find the unknown unknowns requires skilled manual investigation. It is the only way to solve this part of the security puzzle, so vet your security partners before any of this work begins and make sure they're up to the challenge.

Put it all together



Source: Hackable

If you have valuable digital assets that are worth protecting, then you want to make sure you fix your security vulnerabilities before your attackers exploit them. To do that, you need a skilled, external partner helping you by investigating your system with the same malicious viewpoint your attackers would have.

They need to go beyond the basics and execute the advanced tactics. All of them.

If you get the right partner and have them do the right testing, you'll know exactly how to deal with your concerns about getting hacked.

We'll help you meet your cybersecurity training goals: Book meeting

Why you should build security into your system, rather than bolt it on

Carbon monoxide is colorless, odorless and tasteless. You don't even know it's there until it kills you.

You may be facing your own silent killer: your delay. When you postpone security until later in the software development process, that delay costs you enormously in both obvious and unexpected ways.

I get it: you need to develop and release as fast as possible. There's enormous pressure to hit milestone dates. The reality, though, is that security really can't wait. Security is part of what makes a product viable — your customers expect your software system to be secure, and if you fail to deliver on that, you fail your customers. It also costs more and creates massive headaches if you postpone it.

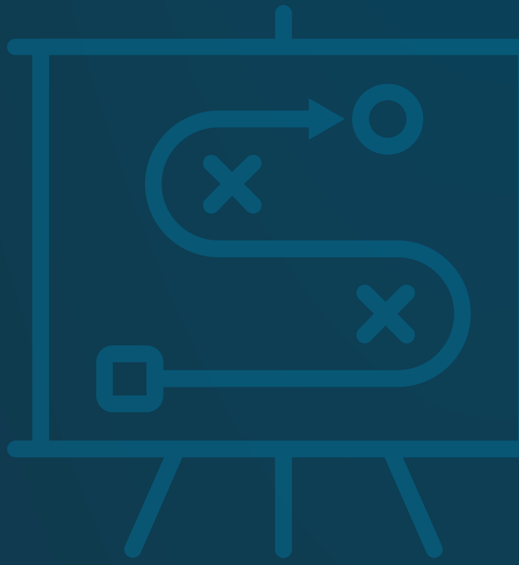
But if you do security earlier in the process, there's a really beautiful upside: not only does that deliver better security, it also makes it easier and less expensive!

"Build security in" vs. "bolt security on"

These concepts have become commonplace amongst the security community, but what's the practical difference between them? The former is when security is part of the development process; the latter is when security is not considered until later.

Consider my friend's incredible roof deck: it has everything you could want, including a grill, big-screen TV and amazing views. But it's missing an important element: a permit.

When he built the roof deck, my friend skipped that step. He planned to come back to it later, but he didn't. Then, when he



We'll help you meet your cybersecurity training goals: Book meeting

tried to sell the house, a buyer's inspection flagged the lack of a permit, which killed the sale.

To get the permit so he could sell the house, he had to overhaul the work he'd already done on the roof deck. It was expensive and took forever. If he had just done it right in the first place, his life would have been so much simpler.

That's what it's like to "bolt security on." It's how most people approach the security of their application, and — like my friend and his roof deck — it's a great way to cause problems for yourself later on.

People simply don't realize it's more expensive and more painful to delay security. But there's a better way ...

Save your company money and effort by building in security

Instead of postponing security to later, make it a core part of your development process. Not only will your system be stronger because you're injecting security into every development decision, but your security efforts will also cost less overall.

You save in two ways: consulting fees and effort. Let's talk about fees first.

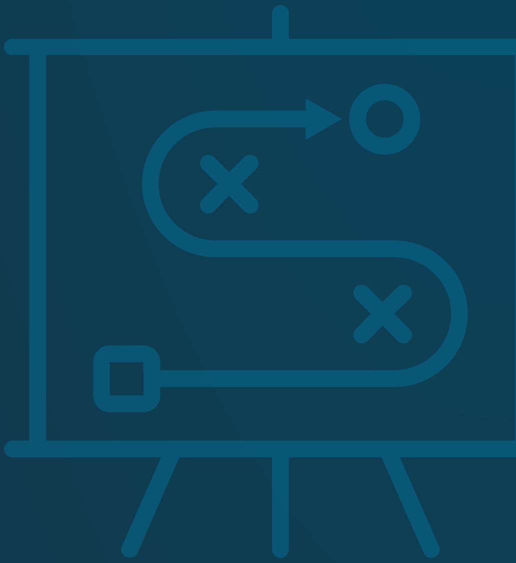
Upon analyzing 13 years of our own security assessment data, we discovered that companies who "built security in" spent an average of 10.1 percent less on consulting fees than those who "bolted security on." That's not mind-blowing savings, but it's real money that doesn't go out your door. Why waste it?

You might not even realize it, but when you push security off until later, you're taking on that waste. You're making it cost more. This costs more because your security partner has to spend more time and effort (which equates to your money) in addressing a higher volume of security issues than if those security issues had been addressed during the development process first.

However, as cool as that 10.1 percent savings might seem, the real benefit comes in terms of your effort. It's easiest to fix a flaw at the moment when it's introduced.

We'll help you meet your cybersecurity training goals: Book meeting

It's easiest to fix a flaw at the moment when it's introduced. It's exponentially harder to fix it later.



It's exponentially harder to fix it later. For example, a flaw introduced in the design phase that isn't addressed until after deployment is going to require a ton more effort to fix. In fact, the data shows it takes 25 times more effort.

25x more effort!

That's bananas. It's pure lost efficiency. It means your developers are spending time redoing work they already did, and are not working on other things to drive the business forward.

Whenever you postpone security, you incur this terrible tradeoff. Every single time. However, when you build security in, you eliminate that effort waste. Just like that, you capture a 25x effort savings. Whose CFO wouldn't love to hear about that?!

So, in summary: when you do it earlier, you get better security, which costs you less in fees and requires substantially less effort.

Make security part of the development process

If my friend had known what a headache his deck would become, he would have secured a permit from the start. Similarly, I encourage you to build security into your development process.

No rational person wants anything to be 25 times harder or 10.1 percent more expensive than it needs to be. Yet, companies do this all the time when they choose to bolt on security.

When you build security in, you convert this waste into efficiency. You save effort, maximize productivity, quickly resolve vulnerabilities as they're introduced or — even better — avoid introducing them altogether.

What does it take to build security into your system? Learn how in my course "Build security in."

Get Started

Is your company testing security often enough?

A crucial component of securing a software system is having independent security experts test it for security flaws. But how often should you have this done?

Short answer: frequently. Probably more frequently than you currently are.

Security is an ongoing process: you'll need to regularly reassess your system for vulnerabilities. If you want to do it right, though, cadence matters. The right reassessment interval for most apps is every three to six months. Some require more or less frequency, but most fall into this range. However, many companies think about security only annually or every two years. Some consider it even less frequently than that.

People tend to follow these inappropriately long timelines because somehow the idea of "annual" testing has become a commonly referenced idea. However, the world changes rapidly, especially when it comes to technology — this inherently changes your security posture since your last round of security testing. Furthermore, attackers are evolving at a relentless pace — if you aren't reassessing your security often enough, it's only a matter of time before they have the advantage.

But it's not too late to get back on schedule!

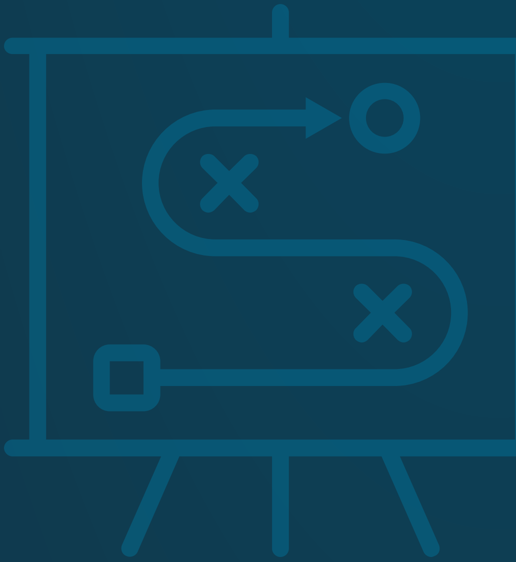
The risk of waiting to reassess

First, let's talk about why you don't want to defer security reassessment for too long.

When you wait too long to reassess your company's application, you undermine your own security mission. For perspective, think back to a year ago, and consider what your technology looked like. Consider what your industry looked like. A lot has changed, right? And don't forget that your

We'll help you meet your cybersecurity training goals: Book meeting

When you wait too long to reassess your company's application, you undermine your own security mission.



attackers have evolved, too. So why would it make sense to wait so long to reconsider security, with that much changing?

It doesn’t.

If you hit the right cadence, you account for change. If you wait too long, you cede the advantage to your attackers. You leave yourself unnecessarily exposed for too long. That can be a costly and avoidable mistake.

Finding the right reassessment cadence

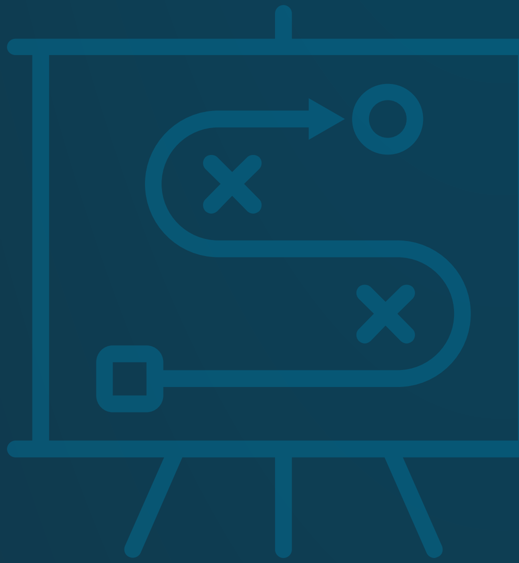
So how often should you perform security assessments?

The time frame between assessments should be driven by a variety of factors, such as how rapidly you develop, how valuable your assets are, how much of an attack target you are and how frequently your customers need assurance. As these factors increase, your time frame between assessments must decrease.

Unfortunately, many companies pace their reassessment intervals on some arbitrary time frame instead. Many people think of security like an annual physical exam with your doctor: a necessary but annoying interruption that you do as infrequently as possible, and hope it doesn’t bring bad news.

Instead, think of security assessments like nutrition: something you consider constantly. You shouldn’t evaluate your sugar intake once a year; you should evaluate it regularly. When you implement an appropriate assessment cadence rather than one that’s too long, you’ll find that it is more effective, and less expensive, too.

Analyzing several years worth of our own security assessment data shows that the best cadence is every three to six months. This is long enough apart so that security doesn’t become cost-prohibitive, but frequent enough that you can quickly eradicate security flaws before they remain exploitable for too long.



We’ll help you meet your cybersecurity training goals: Book meeting

Less expensive, more effective results

The benefit of finding the right assessment cadence is twofold: not only are frequent assessments more effective at preventing attacks, but in the long run, they're also less expensive, too.

When you perform assessments more frequently, you identify and remediate security vulnerabilities more quickly. You reduce opportunities for exploitation, accelerate knowledge transfer from your security experts to your developers and get more opportunities to learn from mistakes. Your developers improve faster and introduce fewer vulnerabilities.

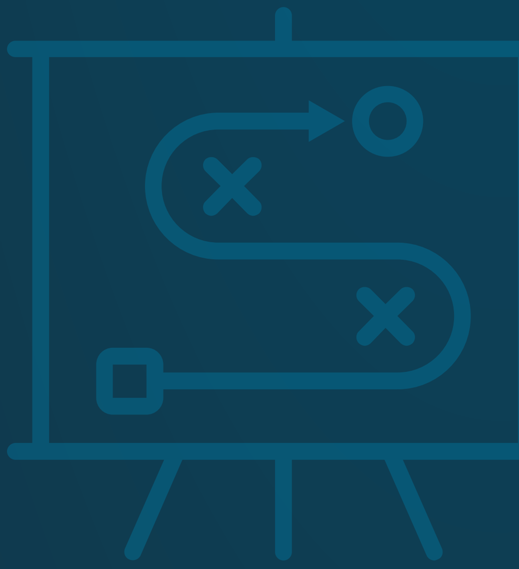
In short, more frequent assessments deliver better security faster.

Security done at the right intervals is less expensive, too. This is because regular security creates efficiencies that accumulate massive savings over time. Your initial assessment is always going to be the most involved effort and thus the most expensive. By contrast, reassessments cost roughly 60% less (if done on the appropriate cadence). If you approach reassessments too infrequently, you're essentially getting an initial assessment every time. But if you hit the right intervals, you get a streamlined effort, which costs substantially less. (For deeper analysis including real-world numbers, see chapter 6 of "Hackable: How to Do Application Security Right".)

Choose the right cadence for your company

Security is a lifetime investment; you'll always be working on it. It will not end. So my advice to you is to invest in the initial assessment just once (and only once!), and don't look back. Avoid the trap of waiting too long, which will result in you paying that higher price every time.

Some companies might need more frequent assessments, some less, but again, the right cadence for most companies falls between three to six months. Anything longer than that, and you risk periods of prolonged vulnerability, which also



We'll help you meet your cybersecurity training goals: Book meeting

makes it harder and more expensive to deal with later.

If you are like most people in technology, you hate waste. You hate inefficiency. When you wait too long, you backslide on efficiency, thereby bringing your costs back up again. Stay on the right cadence, and you avoid that waste and get better results for less money.

Need to know when to reassess your system? Find out more in my course “Hack it again.”

Get Started

Success

GETTING IT RIGHT, REPEATEDLY

> “Your customers want to use software that is secure, and when you can prove that yours is but others can’t, you’ll win.”
>
> — Ted Harrington

How should your company think about investing in security?

Security gives your company a competitive advantage

How to find the perfect security partner for your company

There’s no such thing as “done” with application security

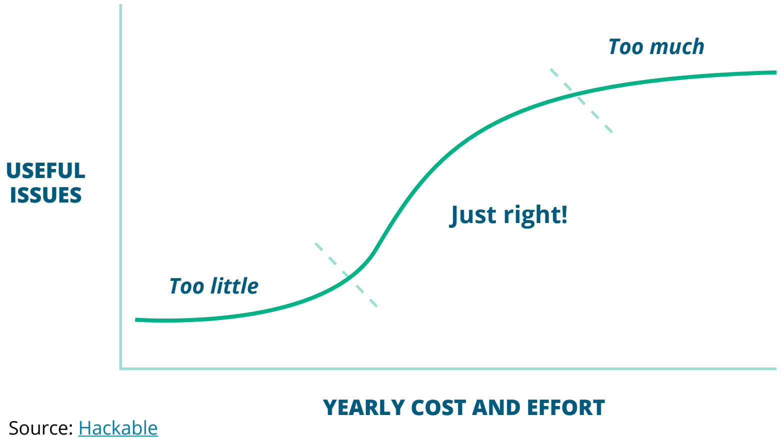
How should your company invest in security?

Like many things in life, with the security of your company's application, you get what you pay for. You can spend too little, too much or just right.

To find the right balance, consider Goldilocks: she goes for a walk in the woods and comes upon a house. In the house, she finds three bowls of porridge. The first is too hot, the second is too cold, but the third is just right.

Goldilocks is the master of figuring out "just right." To determine the appropriate security budget for your company, you need to be, too.

THE GOLDILOCKS PRINCIPLE



Source: Hackable

How much security effort is too much?

First, let's explore the idea of overinvesting in security. How much is too much?

At a certain point with security, you start to see diminishing returns: issues still appear but more rarely. Security is never really "done," so it's tricky knowing when to move on. There's

We'll help you meet your cybersecurity training goals: Book meeting

always more to do, more to find, more to fix. Knowing when to wrap up depends on your threat model, risk appetite and your unique circumstances.

However, your company probably isn't in this category. Almost nobody is. You certainly *can* get there, but you're likely not there now. The takeaway is this: even though you're probably not in this category yet, it's important to know that security is not an endless investment of resources. There is a point at which you can accept the remaining risk and move forward.

The problem with too little effort

On the other hand, companies often spend too little effort on security. Almost everyone falls into this category.

Security is often viewed as a "tax" on the business. Companies want to minimize any kind of tax, and so they try to cut security spending inappropriately. However, most people don't realize that when you cut costs, what you actually cut is effort: how much time you invest, how manual it is, how much attack surface you cover and how thoroughly you develop custom exploits. That's a dangerous elixir because your attackers already invest more effort than you can. Cutting effort just cedes more advantage.

As a leader, you're under tremendous pressure to make the best use of the limited money and person-power you have, and those resources need to cover a wide range of priorities. It's sometimes hard to justify the investment in security, and even when you can, you aren't always sure where the best place to invest it might be.

Here's the harsh reality, though: the less you invest, the less it returns. When you cut costs too far, you prevent outcomes that help you get better. Achieving your security mission is going to cost you time, effort and money. There is no way around that. When those investments get cut to the bone, what's really reduced is your ability to succeed.

The trick to successful application security lies in finding your sweet spot, that magical balance where you uncover useful issues without investing too much or too little.

We'll help you meet your cybersecurity training goals: Book meeting

The level of effort that’s “just right”

The trick to successful application security lies in finding your sweet spot, that magical balance where you uncover useful issues without investing too much or too little. There are many variables that influence this, including:

- The value of your assets
- The skills of your adversaries
- The scope of your attack surfaces
- The amount of risk you’re willing to accept

As a ballpark estimate, to do application security testing right is probably going to cost $30,000 to $150,000 or more per year, per application. Some cost far more than that.

That number might shock you; as discussed, most companies are in the category of spending too little. Security isn’t cheap because it’s not easy, it requires a unique skill set, and it takes effort.

However, doing security right is *worth* the price.

The incremental cost of doing security right is a tiny, microscopic spec compared to the gigantic cost of a security incident. Most importantly, since most companies struggle to do security right, those who do obtain an enormous advantage over their competitors. You want to be one of those companies. To get there, you need to invest appropriately.

There are no security shortcuts

Ultimately, you can’t achieve security excellence by going cheap. You can’t find the unknowns for cheap. You can’t

Want to make the best use of your security budget? Learn how to balance time, effort and money in my course “Spend Wisely.”

Get Started

We’ll help you meet your cybersecurity training goals: Book meeting

discover custom exploits for cheap. You get what you pay for, and there's no way around that. However, you also don't need to spend endlessly either; even though there's always more to fix, there is a point at which you can accept the remaining risk and move on.

The best approach is to channel your inner Goldilocks and find the budget that's "just right" for your company. Figure out how rigorous and comprehensive an assessment your application requires, and don't fall short of those standards.

When you focus on reducing cost, you let the wrong factors drive your security mission; you wind up trying to slash investment. That simply reduces effort and thus undermines your chances of security success. Instead, use the right factors to drive your security mission: what you want to protect, why and from whom. Trust that there is a happy balance that sets you up for success on your security mission, while meeting the financial constraints that exist in every business. Go find that balance.

The best place to start is to establish your threat model, and use that as the basis to determine risk. Once you understand risk, find the appropriate balance of investment that helps you manage it to a level you're comfortable with.

We'll help you meet your cybersecurity training goals: Book meeting

Security gives you a competitive advantage

In rowing, when your team is in sync, the boat is flying on the top of the water, and you're winning — it's pretty magical. But sometimes, you "catch a crab."

A stroke lands at a bad angle, causing the water to rip the oar out of your hands. The oar rams you in the chest, knocking you into teammates. No longer rowing, the oars become brakes. The boat screeches to a halt, and you lose the race every time.

That's how most software companies experience the dreaded part of the sales process: when your customer wants to talk about security. Everyone falls out of sync and stops moving forward. Competitors beat you to the finish. The team is totally demoralized.

But it doesn't have to be that way.

What if instead, security was something that *helped* the sales process rather than *hindered* it?

That's exactly how progressive tech companies approach it, and it's how you should too. When you properly secure your software system and then can prove it, you obtain a competitive advantage that helps you earn trust and win sales.

Security is a differentiator

Every bit of security adds value to your customers. Some security can be considered "table stakes": the basics that everyone must do. Everything else — the things that separate those who do security right from those who don't — are differentiators.

As one chief technology officer put it, "Being clear about our security strategy helps the buying conversations with our customers. They see it as a differentiator."

We'll help you meet your cybersecurity training goals: Book meeting

As someone working deep in the trenches of security, I agree with him. Here's why:

- Most companies don't understand security, let alone how to do it right.
- Most companies don't understand their attackers and don't have a threat model.
- Most companies invest in security too little, too infrequently, with too little collaboration, using the wrong methods focused only on the issues of too little significance.
- Most companies are not secure.

By contrast, companies who are thorough in their security process stand out. When you have a rigorous security assessment process, done at the right cadence and appropriate depth using the right methodology, you're able to secure your application in ways that everyone else simply can't.

Then, you can prove it, which is yet another thing everyone else can't do — because if it wasn't properly secured in the first place, attempts to prove it's secure will fall flat.

Therein lies the magic of security done right: your customers want to use software that is secure, and when you can prove that yours is but others can't, you'll win.

Security earns your customers' trust

To use security to drive sales, you need to get your customer to trust you first. If they do, they buy faster. If they don't, they hit the brakes and proceed with caution.

The opposite of trust is fear. You introduce fear when you make hollow promises, misleading claims and fail to back claims up. For example, every breach notification letter always seems to include the phrase "We take your security seriously." But do they? After all, they were compromised. Is that because they cut corners and didn't invest enough in security? Other nonsensical claims are when people state their system to be "highly secure" but don't explain what that means. Or the granddaddy of hilarity: "bank-level security"

We'll help you meet your cybersecurity training goals: Book meeting

and “military-grade encryption” try to imply this system is as strong as a bank or good enough for the military, but really it just refers to a specific detail (the encryption algorithm).

If you make claims like these, you lump yourself in with all of the other people who don’t know how to do security right.

Instead, you want to build trust. That’s pretty straightforward so let’s not overcomplicate it:

- Tell ‘em your security philosophy. What’s your approach to security and why do you believe in it?
- Tell ‘em what you did, what you found, and how you’ll fix it. What kind of testing are you doing, how often, and what’s on the remediation roadmap?
- Tell ‘em how to verify what you’re saying. Where can they read your security assessment report?

Implement these across your sales process and on your marketing website. Use your security assessment report and leverage your security consultant, too. These things help your customers know that security is a priority for you. They’ll like that.

Customers want to buy from companies that get security right — all you need to do is show them that’s you.

Be honest and open about your security

Serious note of caution, though: none of this works if you don’t actually go deep enough to secure your solution. That is a very important detail, given that many companies don’t go deep enough (and most of them actually don’t realize it). You simply can’t prove you’re secure if you’re not actually secure in the first place.

However, if you are going deep enough and you are secure, you gain a competitive advantage. To earn your customers’ trust, just be honest about your security efforts.

Security is not a trick. There’s no need to mislead or make unsupported claims. Just be frank. Be straightforward about

what testing you're doing and why. When you ask questions of other people, you want them to give you the straight truth. That's exactly what your customers want from you, too.

Remember, many of your competitors likely fail to address security properly, so differentiate yourself. Seize the competitive advantage available to you. Start by properly securing your system, and then prove it. These things will put you on the fast track to earning trust — and trust leads to sales.

Looking for ways to beat your competitors? Learn actionable tactics and how to use them in my course "Use security to win sales."

Get Started

How to find the perfect security partner

An external security partner provides a valuable service: security testing, paired with objective advice on how to keep your applications secure. They often make the difference between protecting your data and suffering a breach, and that means you don't want to hire just anybody — you want to hire the *right* security partner for your company's needs.

Not all advisors are created equal, so you'll want to choose carefully and consider a variety of factors: Do you need a product or a service? A tool-centric or human-centric partner? What specialization does your company need?

Different companies have different security needs, and by gaining an understanding of the main differences between security providers, you can select the right partner to protect your assets.

Products vs. services

First, you'll want to decide what form your security solution should take. There are three types of security companies: companies that sell only products, companies that sell only services and companies that sell both.

Assuming your goal is to find and eradicate security vulnerabilities so you can build secure software systems, that goal requires an *advisor*. By definition, that's a service, so you can rule out product-only companies (note: you will need products too for aspects of your security program; but for the sake of this article, we're just talking about the testing and advisory aspects). Furthermore, be leery of companies that sell both services and products if those services result in buying their product. For example, their consulting might inform you of a security issue that *just so happens* to be solved by a product they sell. That brings into question the integrity of the recommendation in the first place.

A security company might be incredibly skilled at what they do, but if they aren't a great match for your company's needs, they won't be your best choice.

We'll help you meet your cybersecurity training goals: Book meeting

For these reasons, I'd recommend you look for a company that only sells services (or sells services and products as long as the products are not the solution to the problems the service will discover). This way, you can trust that the advice they give you solves your problems, and isn't distorted by a motivation to sell a product.

Tool-centric vs. human-centric

Second, once you've identified a few security-partner candidates, figure out whether they offer a tool-centric or human-centric service. Many "service" companies are just running an automated tool and presenting it as a service. You can't scan your way to security excellence.

Instead, you want to find an advisor who has smart, experienced experts who can help you solve your problems with the creativity that comes with being a human. The work needs to be manual.

To find the truth about a company's service, ask questions: Is their advice personalized? Who does the work? What are their qualifications? How much is automated? What data and reports will you receive? Dig until you understand exactly what you're paying for.

What is their specialty?

Lastly, after you've narrowed down your candidates to just a few options, you'll want to focus on their specialties. Make sure their area of expertise aligns with your business's needs.

Some companies will present themselves as experts in *everything*. Be wary of that; no one is the expert in everything. Most companies, however, do have a specialization, even if they have a wide range of capabilities. Ask what their single strongest area is, and that should help guide you.

Vet the companies' qualifications to ensure that they're as good as they claim to be. Look for research they've published, talks they've given at industry conferences, documentation on their methodology, and the deliverables they give to clients. If any of these are lacking or missing altogether for a given security company, consider ruling them out.

We'll help you meet your cybersecurity training goals: Book meeting

Find the right security match for your company

A security company might be incredibly skilled at what they do, but if they aren't a great match for your company's needs, they won't be your best choice.

Remember, as an external partner, it's not just about security testing: this company will also serve an advisory role in guiding your company's security practices. Like a personal trainer, they apply years of experience. They point out where your form is bad and help you fix it. They hold you accountable. They make you better.

For the best results, choose a service-based, human-centric company that specializes in the area you need most. Look for these traits, and you'll find a partner who can help you achieve security excellence.

Need help finding a perfect security partner for you? Leverage your in-house expertise and accelerate your efforts with my course "Start with the right mindset and partner."

Get Started

We'll help you meet your cybersecurity training goals: Book meeting

There’s no such thing as “done” with AppSec

If you’re like most companies in the software business, you’re relentlessly developing new features, streamlining workflows and improving the user experience. But every single change to your platform also changes how you might be attacked. As you develop new code, you’ll almost certainly inject new vulnerabilities. Those need to be addressed.

Technology evolves so quickly that it requires you to constantly revisit your security to stay ahead of new vulnerabilities. The process never ends. As one director of application security described it, “Once you know the rules, the game changes.”

The best way to deal with this is to treat security as a cycle, a process that continually repeats. However, many people tend to think of security as a one-and-done process, something that is linear with a start and finish, after which it doesn’t need attention again.

But that’s wrong. Security is not a line; it’s a loop.

The only constant is change

Change is inevitable.

For example, your customers’ demands change. Sometimes they require new security controls. Sometimes they want to change their model, such as moving from software that is hosted on-premises (which runs at their physical site on computers they own and control) to software that is cloud-hosted (which runs remotely on computers owned and controlled by a service provider). Whatever the change, they need assurance that your security meets their new needs.

Another type of change is the invention of new attack techniques. Attackers are just like you: they’re constantly innovating. They’re relentless in inventing new ways to exploit systems. You need to constantly investigate these new techniques, too. Security truly is an arms race, and you need to keep up.

We’ll help you meet your cybersecurity training goals: Book meeting

Security is not a line; security is a loop. Yes, there is a process, but once you finish, you must repeat it. Forever.

Lastly, widespread vulnerabilities in core technologies are discovered. The very nature of building software is that you'll have dependencies. Whether that's on a cloud provider, third-party libraries, integration of third-party solutions or some other shared component, your security relies on someone else's security to some extent. Those third parties are evolving, too, while at the same time, new exploits are discovered in them.

Change happens all the time, and you need to reevaluate your system to defend accordingly.

Take a lesson from the ultimate hackers

Change impacts your security, and to deal with that, you need to adapt. You want to be like nature's ultimate hackers: squirrels.

If you've ever seen a bird feeder, you've seen squirrels defeat almost any attempt to prevent them from stealing the feed. Squirrels don't care that the feed isn't for them. To the squirrel, it's about survival — steal the feed or die. So they relentlessly adapt to whatever barrier is thrown at them.

With application security, you're up against the same level of intensity. Like squirrels, your attackers will stop at nothing to break the rules of your system, exploit functionality and gain access where they don't belong. That's how your attackers think, and that's how you must, too, if you want to defend against them.

An iterative approach to security

All of this change requires that you take an iterative, ongoing approach to security.

Many people mistake security as being a linear process. Do step A, then step B, then step C and you're done. But that's wrong. Security is not a line; security is a loop. Yes, there is a process, but once you finish, you must repeat it. Forever.

We'll help you meet your cybersecurity training goals: Book meeting

The process follows a simple formula:

- Establish/update your threat model
- Perform security assessment
- Remediate your vulnerabilities
- Continue developing but with security in mind
- Repeat

As a senior vice president of product management put it, “There’s no finish line for security.” You will refine your process, but it will never end.

Reassessments keep your application in the clear

The best way to do this is through what’s called reassessments. They entail the ongoing process of evaluating your system for security vulnerabilities, so you can continue to improve it. Eradicating vulnerabilities is the point of security testing, and given all of the ways the world is changing, vulnerabilities will continue to appear. Reassessments ensure you continue to identify them so you can fix them.

Therein lies the value of reassessments. Even though you’ll introduce new vulnerabilities as your application inevitably changes with time, you’ll be able to catch them. Reassessments help you deal with change, identify the new vulnerabilities that get introduced over time and ultimately keep your system as secure as it can be.

You’ll never be “done,” but you will be building a better, more secure software system.

Looking to minimize costs and maximize your security impact? Check out my course “Hack it again” and discover the best cadence for your organization and the business outcomes obtained from doing it right.

Get Started

We’ll help you meet your cybersecurity training goals: Book meeting

Additional resources

Train your team

- Upskill your IT, security and engineering teams
- Earn and maintain your team's certifications
- Build hands-on experience through realistic cyber range scenarios
- Assess your team's skills

More from Ted Harrington

- Take Ted's Infosec Skills learning path, How to Do Application Security Right
- Watch the Infosec Edge webcast on How to Do Application Security Right
- Get Ted's book, How to Do Application Security Right
- Read Ted's articles on Infosec Resources
- Watch Ted's Cyber Work Podcast episode

More from Infosec

- Cyber Work Podcast
- Infosec webcasts and events
- Infosec YouTube channel
- Infosec Resources blog

We'll help you meet your cybersecurity training goals

Book meeting

About Infosec

Infosec believes knowledge is power when fighting cybercrime. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and privacy training to stay cyber-safe at work and home. It's our mission to equip all organizations and individuals with the know-how and confidence to outsmart cybercrime.

Learn more at infosecinstitute.com

INFOSEC™