CONNECTWISE

CONNECTWISE EBOOK SERIES

The Birds, the Bees, and the Breaches:

HAVING THE CYBERSECURITY CONVERSATION WITH YOUR CUSTOMERS

CONTENTS

INTRODUCTION

Whether You Know It or Not... YOU Have a Security Problem

Most SMB's lack an understanding of IT, let alone security. Everything to your customer is an IT problem. They believe you are accountable for 'all' security issues, and they're not very accepting of adding costs for a level of security they believe you're delivering. Moreover, as a technology service provider (TSP), you could be held liable in the event of a customer breach.

That's a problem.

In truth, there is a chasm caused by the disconnect between what services you know are being provided and what the customer assumes are being provided. The chasm is widened because of a language barrier—the cybersecurity language. In order to have effective dialogue with your customers, it's important to establish a common language to truly educate and communicate with them on new and emerging security threats.

Our goal is to give you a framework and insight to have consistent, effective, and valuable conversations about advanced security services with your customers. The desired outcomes of these conversations include raising awareness, resetting expectations, aligning the services you provide with the proper pricing, growing your security offerings, and helping to protect you in the event of a breach.

CHAPTER 1: WHY HAVE THE SECURITY CONVERSATION (AND NOW)?

Why This Is Necessary for You

There are three critical reasons to engage in security conversations with your customer. Assumption of risk and protecting yourself, increased revenue opportunities, and preventing loss of business. We'll go into each of these reasons to explain why action is necessary and why inaction is not an option for you.

1. You're Holding the Keys to the Castle

TSPs have become a frequent target as of late. APT 10 Hackers are breaching SMBs by exploiting vulnerabilities and infiltrating their TSPs. However, most TSPs are not doing internal risk assessments, vulnerability scanning, or have a third-party Security Operation Center (SOC) monitoring their own infrastructure and data. Nor do they have security policies in place that are regularly reviewed. This is not a very strong or defensible position, should the TSP need to defend themselves if their customer experiences a breach.

Think about it. If you were a criminal, what's more lucrative: stealing a single Maserati out of someone's driveway or stealing a trailer full of them?

2. Customers' Perception is Reality

In polling over 500 ITSPs, when asked; do you believe your customers think you (the TSP) are responsible for all things cybersecurity related? Over 90% answered is 'yes.' Next question we posed; are you responsible for all things cybersecurity related, based on what you are being paid for today? Over 90% said 'no.' Last question; what are you doing about the diametrically opposing beliefs that you and your customer have?

Answers are as follows:

72%

Nothing – I do not want to have the conversation, because they will ask why they need to pay more, when I sold them on a Managed Services Agreement, that says 'we do it all.'

(We'll show you how to address this later in the book)

20%

"We updated our contracts" – the belief here is, if the TSP updates their contract that indicates they are not responsible for certain aspects of cybersecurity, they are not liable. This is not always the case, in fact, without proper assessment of risk, sharing this with your customer and having them sign an attestation letter (attest) that they own the risk, you in fact could be negligent.

8%

We are maturing our service offerings, adding risk assessments, becoming more knowledgeable about who owns the risk, and changing our sales and vCIO review processes.

Over the last 10 years, most TSPs have offered what some refer to as IT security services as opposed to cybersecurity services. IT security would include antivirus/anti-malware, email protection, firewall protection, etc. And for a while, there was nothing wrong with that. Now it only captures a fraction of the critical security controls.

Threats today are more advanced and become more sophisticated every day. The result? There's a growing divide between the threats your services protect against and the advanced threats that exist today. The problem today isn't only limited to the technology...it's the people!

Remember, for the past 10 years, you've pitched your service to say, "We're your trusted advisor, we align your business with technology, we reduce your risk and exposure, and we do it all for one monthly price."They were sold on your expertise on all things IT, and when something is wrong, the expectation is that you'll take care of it. There have been cases where a business has been hit with ransomware, and when it couldn't be reversed, expected the TSP to pay the ransom. Several of those times, the TSP did, in fact, pay it. Incurring that cost can be crippling to a TSP, and not paying it can be catastrophic to their reputation, so it can be a no-win scenario.

Having this conversation with your customers will enable you to set expectations of what services are covered by your service agreement, where the gaps are, and discuss options to remedy those gaps. This will also help establish who is responsible in the event of an incident. This leads to our next reason to have this conversation.

3. Increased Revenue Opportunities for You

Mitigating risk is one possible outcome, and there is a benefit to both you and the customer. For you, it lowers your ticket counts, and for your customer, it lowers their risk and potential business interruption.

By identifying the products or services missing to meet a security control, you can reframe the narrative to two basic concepts:

- The customer sees the need for increased services, and will pay you as such
- The customer sees the need for increased services, and There will be a clearly defined list of services that you are responsible for, and a list that the customer is responsible

At worst, you've mitigated the risk of threats you don't protect against; at best, you've increased your services, as well as your MRR.

However, if you're not talking with them, you can bet that other competing TSPs and MSPs who are asking for their business ARE asking them about their current security services. Not addressing this head-on can result in lost segments of the customer's business, or, ultimately, loss of business from that customer entirely. You're holding information that your customers need to hear. However uncomfortable it may be, it's better to address the elephant in the room than have the conversation after the fact where your customer says, "Had you told me this was an issue, we could've done something about it."

CHAPTER 2: THE CONVERSATION YOU SHOULD BE HAVING, BUT LIKELY AREN'T

Whether you realize it or not, the cybersecurity landscape today puts you squarely in the Risk Management business.

Just like a life insurance agent, it's your role to advise your customers on their current position, their greatest areas of risk, and how to offset the risks they carry today. As the trusted adviser, the critical question you should be asking your customer is:

> *"What risk level are you willing to accept to protect your most valuable assets?"*

The crucial conversation today is about clarifying your customers' security risks as they stand today, where they need to be, and getting on the same page about how to tackle them. The name of the game is keeping their intellectual property and critical data safer, which only comes from understanding their current risks and vulnerabilities and fortifying their defenses against cybercriminals to get to a more desirable risk position.

To be clear, this is not a technical conversation, but a business conversation.

Let's look at how to bridge the security gap between you and your customer to make the conversation productive.

The Need for a Common Language

Think back to the first time you went to a Starbucks. You learned that what you call a small coffee is known as a 'tall' there. When you said you wanted skim milk instead of whole milk that it was referred to as 'skinny.' Terms such as 'no whip,''extra shot,' or 'drip' that at once felt foreign and clunky, are now second-nature to you. Once you learned this language, you can now walk into any other Starbucks, communicate perfectly, and get your beverage consistently.

Why do this? Frameworks make complex information more digestible.

For Starbucks, it was a way to handle a wide array of customized orders while increasing efficiency that could be replicated across all of their locations, while providing a consistent experience for their customers.

What is the common language when it comes to cybersecurity? The language we recommend is based on the National Institute of Technology (NIST) Cybersecurity Framework.

The NIST Cybersecurity Framework

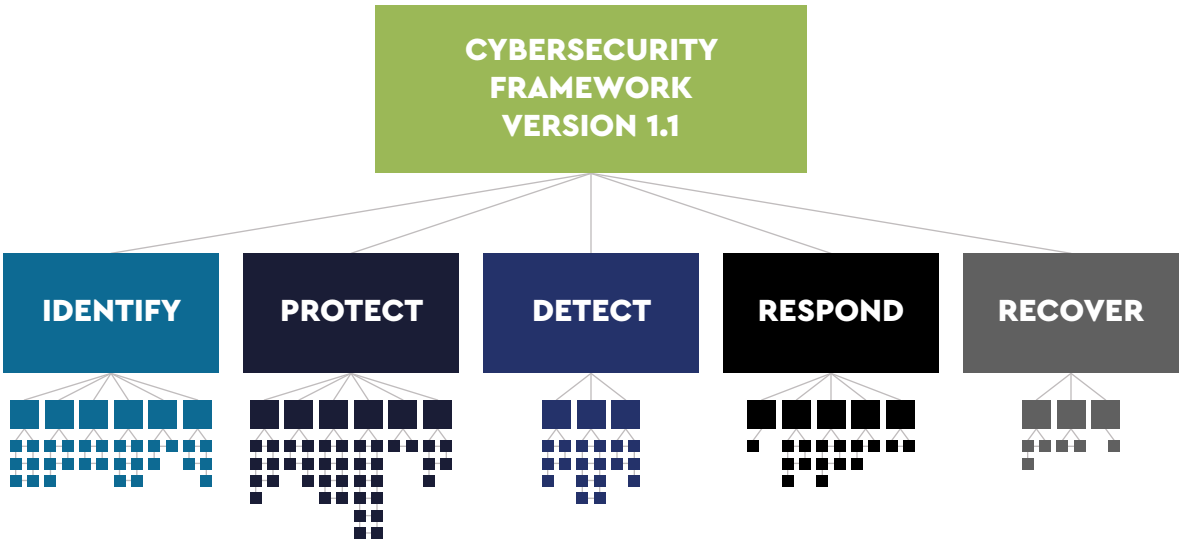
Cybersecurity is a global problem. Attacks originate from many countries around the world. With so many computers controlling so many elements of our society, including banking, energy, hospitals, law enforcement, and the military, cybersecurity is more than a business safeguard, it's critical to national safety. Establishing a common platform is a vital step towards helping to assure the security of people and business around the globe. That is where NIST (National Institute of Standards and Technology) enters the picture.

NIST is a US Government agency whose metrics and frameworks support the smallest of technologies to the largest and most complex. They have created the Cybersecurity Framework, which is a robust and specific set of controls designed to help SMBs assess their strengths and vulnerabilities and improve their security posture. Moreover, it helps to ensure consistency by giving everyone a common language to speak and measure themselves.

There are hundreds of frameworks across the globe covering industry specific areas. NIST's approach to the Cybersecurity Framework is broad enough to cover a wide range of governance. Hence the reason it has gained in popularity as a starting point to the cybersecurity conversation.

Exploring the Framework: Functions, Categories & Controls

As you can see from the previous illustration, the framework is divided into five functions: Identify, Protect, Detect, Respond, and Recover. Those functions then expand into categories that makeup each function.



There are presently 23 categories within the framework.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
1. Asset Management	1. Access Control	1. Anomalies & Events	1. Response Planning	1. Recovery Planning
2. Business Environment	2. Awareness & Training	2. Security Continuous Monitoring	2. Communications	2. Improvements
3. Governance	3. Data Security	3. Detection Processes	3. Analysis	3. Communications
4. Risk Assessment	4. Info Protection Process & Procedures		4. Mitigation	
5. Risk Management Strategy	5. Maintenance		5. Improvements	
	6. Protective Technology			

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. There are currently 108 security controls that map back to the categories. These controls cover a broad range of topics including asset management, endpoint management, governance, data protection, etc.

To dive deeper into the full breakdown of the framework, you can download it for free from the NIST website here. Familiarizing yourself with it and its components are necessary to help establish a common language with your customers, as it's essential to having conversations regarding your customer's security posture and options.

Using the Framework to Assess Risk

Now that you understand the controls that make up the framework, you can see how it can be used to assess how secure any company is. Does company X have managed remote access? Check. Asset vulnerabilities are identified and documented? Check. Are external information systems cataloged? Nope.

Using the Cybersecurity Framework as a benchmark makes sense because it's objective, measurable, comprehensive, and consistent. It works across any industry, allows you to compare one company to another easily, and gives context when telling a customer how they compare to their industry.

Simplifying the Risk Conversation for SMB Owners & Executives

The NIST Cybersecurity Framework is a lot to digest. Think about how much time you've had to spend studying different compliance models or regulations to get a good level of understanding.

Your customer needs the Readers' Digest version that doesn't overload their brains with technical jargon.

What they need to know is:

1. The Problem: What is the risk?
2. The Importance: What is the severity of the risk?
3. The Solution: What can we do to solve it?
4. The Costs: How will this impact my business if we do nothing vs the solution?

This is a practice that should be done consistently with every customer. By leveraging a risk assessment platform, you can tangibly show what risks need to be prioritized based on the potential impact of gaps in their current operations.

ConnectWise now offers a risk assessment tool to make risk assessments a repeatable part of your customer experience. After addressing critical questions around the NIST Cybersecurity Framework with your customers, you'll get a report of each customer's overall risk level, and the top risk areas to address first, as well as steps needed to remediate those risk areas. It also then produces a very user-friendly report that anyone can understand.

CHAPTER 3: HOW TO APPROACH THE CONVERSATION

Now that you're armed with the objective, concrete assessment of your customer, you have the basic components necessary to have a productive security conversation with them. The big question is...exactly HOW should that conversation go?

We showed you earlier that over 70% of those service providers we polled have NOT had the security conversation. These are some of the questions that have kept them from doing it thus far:

- Where do I begin?
- What should you say vs. not say?
- Is my customer going to be upset because they think I'm not providing the services they expect, or because I may ask for more money?

The end goal of the conversation is to establish what you've been responsible for with regards to security, educate your customer on their security posture, and come to an agreement of either re-defining services and costs for services and/or documenting who is responsible for what in case of a security incident or breach.

In order to have an effective conversation with your customers, there's a general narrative flow. That flow consists of:

- **Setting the Table:** Share stats, news stories, anecdotes, etc. Educate about SMBs being vulnerable, just like big companies.
- **The Changing Landscape:** Explain how changing threats require new safeguards. Introduction of the NIST Cybersecurity Framework and the assessment.
- **Turning Negatives Into Positives:** Explain the difference between the services you've been offering vs. new services without it being perceived as a lack of service or value.
- **Setting Expectations:** Redefine clearly where your services start and stop. Decide who is responsible for what in the event of an incident.
- **Justifying Additional Services:** Position additional fees for additional services. Make the case of offsetting costs from savings due to better protection.

Setting the Table

Have often have you heard your customers say, "It'll never happen to me"?

Customer ignorance is the biggest hurdle to buy in, which is why the introduction to your conversation needs to pack a punch. Your goal here is to put the conversation into a context that directly relates to what they care about.

Since most of the high-profile cases people read about are large companies (Equifax, Apple, Target, etc.), they may have it in their mind that large companies are the targets, and they're immune or safe from new threats. This is your opportunity to prove to them that attacks on SMBs are real, on the rise, and can pack a devastating blow.

Do your research to make it relatable to them, pulling from recent news stories or stories regarding companies in their industry or geographic region. For example:

- 43% of cyberattacks target small business.
- Only 14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities, and attacks as highly effective.
- 60% of small companies go out of business within six months of a cyberattack.

Ask hard hitting questions to get them thinking about how prepared they would be if an attack happened to them:

- Recovery fees
- Fines (often per record)
- Legal fees
- The embarrassment of telling their customers their data had been compromised
- Severe reputation damage
- The hassle and stress of an investigation

The Changing Landscape

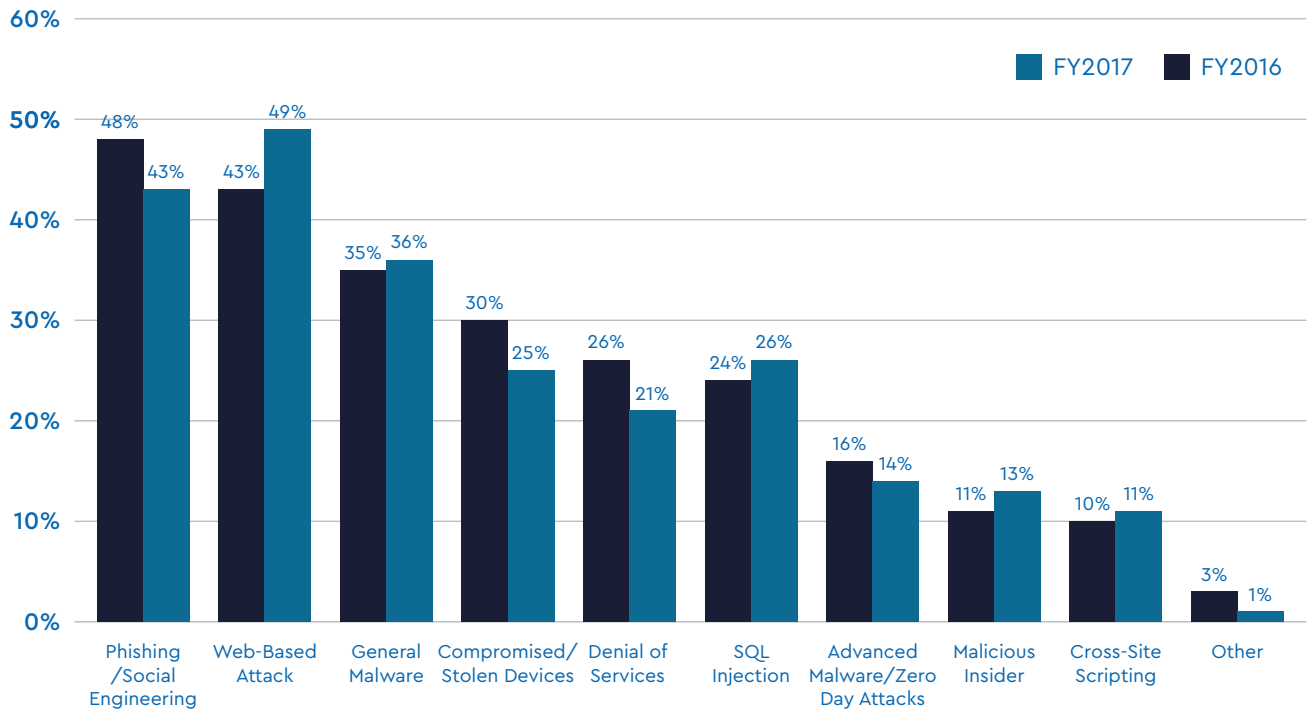
After establishing a mutual recognition of attacks and the negative impacts that can result, this segues nicely into the next part of the conversation. The goal is to portray that you and your customer are on the same side of the problem—a rise of more sophisticated cyberattacks and the increase in action to safeguard them to a level of their comfort.

Security was a modest part of the services that you've provided until now; cybersecurity is now at the forefront of business IT needs. Endpoint protection, firewall protection, and email protection were staples of the managed services business, but they're simply not enough anymore. Failure to address these increases the chance of a serious security event, and reduces the chance to avoid downtime, a work stoppage, or worse.

Include stats and stories relevant to their industries, their customer's security, and/or compliance. For example, "These new threats don't merely impact you, but your customers, your suppliers, etc. If someone were to breach your company, it could give them access to your critical systems and data. Similarly, Ms. Medical Company, an incident cannot only cause a loss of business to you, but compromise your patient's protected data, and be in breach of HIPAA requirements."

What's Behind The Trends: Attack Vector

What types of attacks did your business experience?



It's at this point that you need to introduce hard hitting proof that they're sitting on risk. "In order to make sure we're as protected as we can be, I went ahead and did a risk assessment of your business to help determine your security posture. The assessment is based on the Cybersecurity Framework created by the National Institute of Standards and Technology, and it's the benchmark we all use to grade all companies, regardless of size or industry."

> *"Add an extra layer of credibility if you can say, "It's the same assessment I perform regularly on my own company."*

The truth is, your job as their TSP is to stay in front of threats that can hurt them. You know that a new standard needs to be set to defend against the new level of threats. It's the reality of the situation we're in today. When you're clear on the minimum standards you feel comfortable with, you can show your customer how serious you are about what's necessary to protect them.

Turning Negatives Into Positives

Odds are that so far, you and your customer are agreeing on most of what is being said here. In their mind, they're likely thinking, "Yes, of course I want to keep my business secure and protected."Then comes the part where the alignment starts to split, "Good thing I'm paying you every month to take care of all this stuff!"

If you remember what we discussed earlier in our poll, most customers believe that their service provider is responsible for ALL things cybersecurity related, and that they're already paying for that service. In that same poll, most service providers acknowledge that they're NOT doing all security services, and that they're NOT being paid to do it. This disconnect can seem negative, which can lead to a lot of questions from your customers.

It's not about creating FUD: Fear, Uncertainty, and Doubt. The key to this conversation is communicating that you're here today not because this conversation is easy, but because it's right. The truth is, advanced threats have created the need for advanced security, and it can't be solved by technology alone. A true trusted adviser is honest about the reality that their customer is facing. Awareness is the first step to intelligent action. And not just awareness of a security gap when an incident happens but taking a wider lens on the organization as a whole before narrowing in on the top problems. By proactively having the tough conversation, you're showing them that you're in it together.

Speak to the non-technical aspects of their business that impact their security posture.

Here's a useful analogy: Home Security. You could put 4k cameras in every room, elaborate sensors on every window, 24-hour monitoring services, etc. If someone inside the house leaves the window open or unlocks the door from inside, it renders all those other measures useless.

You can also explain that some of these additional safeguards don't require constant monitoring. Some are initially created and reviewed quarterly, or yearly (such as policy management or security awareness training). If a customer doesn't wish to, they don't have to spend another dime on their services with you. However, they are now aware of risks that they are potentially exposed to, and you can reframe where the line is between what you're responsible for vs. what they're responsible for, which we'll cover next.

Re-Setting Expectations

Part of this conversation is ultimately about who owns the risk. Ultimately, for each risk that is identified, there are three options your customer can take:

1. **Mitigate the Risk:** Putting mesures in place to address it (you and/or your customer)
2. **Transfer the Risk:** Process by which organization pass risk onto another entity
3. **Accept the Risk:** You have identified and logged the risk, but you take no action

By using a risk assessment report to start this discussion, you can establish a new baseline of the services you are, and more importantly, are not covering, putting the onus of responsibility back on the customer to accept or refuse solutions to address the risks.

Here's a very relatable analogy to illustrate the point:

When you bring your car in for service or maintenance, they'll run a diagnostic and/or multi-point inspection (an assessment) on your vehicle. They may tell you that you need to have your brake shoes replaced. With that service, they also recommended to do a brake line flush. You don't HAVE to do it, but not doing it runs the risk of a bigger problem. On a different area of your vehicle, they point out a borderline low tread with your tires. They tell you that action isn't necessary at this point, but keep an eye on it, and eventually you'll need to replace them. You tell them to do the first service but refuse the second one. When you pay them, you'll see on your receipt something like 'customer declined service.' In this case, the service company has eliminated the risk related to the brake service and remediated the risk on the tires. Also, by you declining the brake flush, you're accepting the risk if something should happen as a result to the brake lines.

If we're applying this back to your conversation, it would go something like this, "After going through your most recent risk assessment, we found a few things that were concerning. Here are our recommendations to address them and protect your company better. You can accept the solution or accept the risk. It's up to you how much risk you feel comfortable with if an incident happened tomorrow."

This will vary from risk to risk and customer to customer, and there are a lot of factors that will determine each action. Budget is a factor. Depending on the severity of the risks, prioritizing them is a sound strategy; a customer may realize a threat, and agree with your assessment, but may need to address more pressing risks first. As we discussed earlier, not all problems are technology-driven, but people- and policy-driven. Security awareness training for a company's employees, as well as education to their disaster recovery plan is as important as a threat detection system.

In the end, remember: This process is a win-win for you.

This is the chance for you to reset or reaffirm where responsibilities and liabilities lie for both you and your customer. Even if it doesn't lead to an increase in revenue, it will strengthen your relationship with your client, and define your service set in this new threat landscape. It will also educate your customers, promote awareness, reduce the likelihood of incidents, and reduce support and ticket counts as a result.

Justifying Additional Services

The toughest part of this conversation is often asking for the sale. However, if you've followed the steps to this point, you've set the stage for a new level of understanding between you and your customer.

The output of a risk assessment is meant to be consultative, informative, and educational. Their first risk assessment will likely have a mix of free and fee-based remediation steps to improve their risk posture. Some remediation steps you can offer at no charge (i.e. helping them write security policy), some will result in a one-off fee (i.e., security awareness training), and some you may recommend rolling into your managed service agreement for an adjusted fee (i.e., threat detection).

When done proactively, this helps you build goodwill with your customer that you're not just here for a handout and you're serious about doing what's right to keep them safe. If they are serious about taking protective measures, they will understand when it comes at a cost.

Another avenue to approach this is discussing the ROI of offsetting their costs by adding these people, processes, policies, and technologies to their current service level. If you covered the cost of a business outage as a result of a successful breach, remind them here that what they're spending per month more than offsets incident prevention or response. Improved policies and an educated staff also save in service tickets. Training smart employees to avoid phishing scams or to protect your data in outside environments will also result in savings that far outweigh the monthly costs. If they're considering cyber insurance, improved security posture will make them more insurable, and reduce their premiums. And finally, making them compliant within their given industry helps protect them in case of any issues that may arise and possibly avoid fines or litigation.

Partners vs. Prospects

Talking about security with an existing partner is more difficult than with a prospect. You're able to approach a prospect with a blank slate and no prior assumption of responsibility.

When having the security conversation with a prospect, remember:

- Ask them what their current security posture is, when their last risk assessment was performed, and what the results were. Their current TSP might have avoided these conversations, and that's an opportunity for you.
- If they don't have an answer, ask, "Why haven't they?" Follow up with the importance of risk assessments and provide them a risk assessment for free. Guide them through the process and explain the NIST Cybersecurity Framework as the industry standard.

This will differentiate you from your competitors—and their current TSP.

It will illustrate your level of service offerings and help justify the charges involved and helps establish credibility and expertise.

CONCLUSION

By now, you should understand how important it is to have security conversations with your clients. It's easy to put it to the side and hope that everything will work out, but when, not if, a cyberattack or data breach occurs, you can't rely on good intentions. Your clients will be looking to you for answers. The first step to having the answers is with a comprehensive risk assessment of their entire business, not just their network. Ensuring that all risks are identified and remediation actions are put into place will put you on the right track on the security journey.

Start performing risk assessments today with your free trial of the ConnectWise Identify® risk assessment platform. Get two free risk assessments—one for your business and one for a client—and start having smarter security conversations.