THE KILLER PROSPECTING QUESTIONS FOR SELLING CYBERSECURITY

The Attention Grabbing, Emotion Stirring, Proven Questions To Ask Prospects & Clients

How Do I Sell Cybersecurity?

It is a very common question with many great answers. One of the first steps you must take if you wish to sell cybersecurity to your customers and prospective customers is **to** ask great prospecting questions. A great prospecting question will make your customer stop... think... and then self discover a problem or pain that they may not have realized existed. It will spur meaningful dialogue and generate opportunities for you to offer help - which ultimately leads to quota retiring, business growing sales. This guide contains 9 Killer Prospecting Questions for Selling Cybersecurity. Learn them, put them into practice and then love the results!

Question 1: If you were hacked today, what would you do next?

This question is designed to invoke an emotion of fear and help your customer realize just how unprepared they are to properly deal with a cybersecurity incident.

Many times, the response may be "I don't know what I would do next?" Or, the response may be incomplete in nature like, "I would call my IT provider."

Either way, you will have an opportunity to discuss the consequences of not being prepared to respond and recover from a cybersecurity attack. You can remind your customer that there is very good chance they will have to deal with a cyber incident one day and that it is imperative to create an incident response plan, train a Computer Emergency Response Team (CERT) and be assured that their DR / BCP plan will work.

You can also ask secondary questions about:

- Incident Response Planning
- Data backup and recovery
- DR / BCP planning
- Breach notification laws
- Insurance coverage and proper Legal Counsel

Question 2: Have you suffered from a cybersecurity incident or breach before?

If the answer is YES then you have an opportunity to learn about the incident or breach. Your customer will relive a troubling experience and you can discuss what was specifically done to prevent future incidents. You may find that your customer hasn't really reduced their risk of getting attacked and that they need your help before they fall victim again.

If the answer is NO then you have an opportunity to discuss the likelihood of them experiencing a cybersecurity incident or breach in the near future. Help them understand their unique exposure given the industry they operate in and the lack of security controls they have implemented and working. Take the liberty to explain how easy it may be for a malicious attacker to succeed and what the consequences may look like.

You should have plenty of reasons to use this question as a great conversation starter about your customers' cybersecurity program and its overall effectiveness.

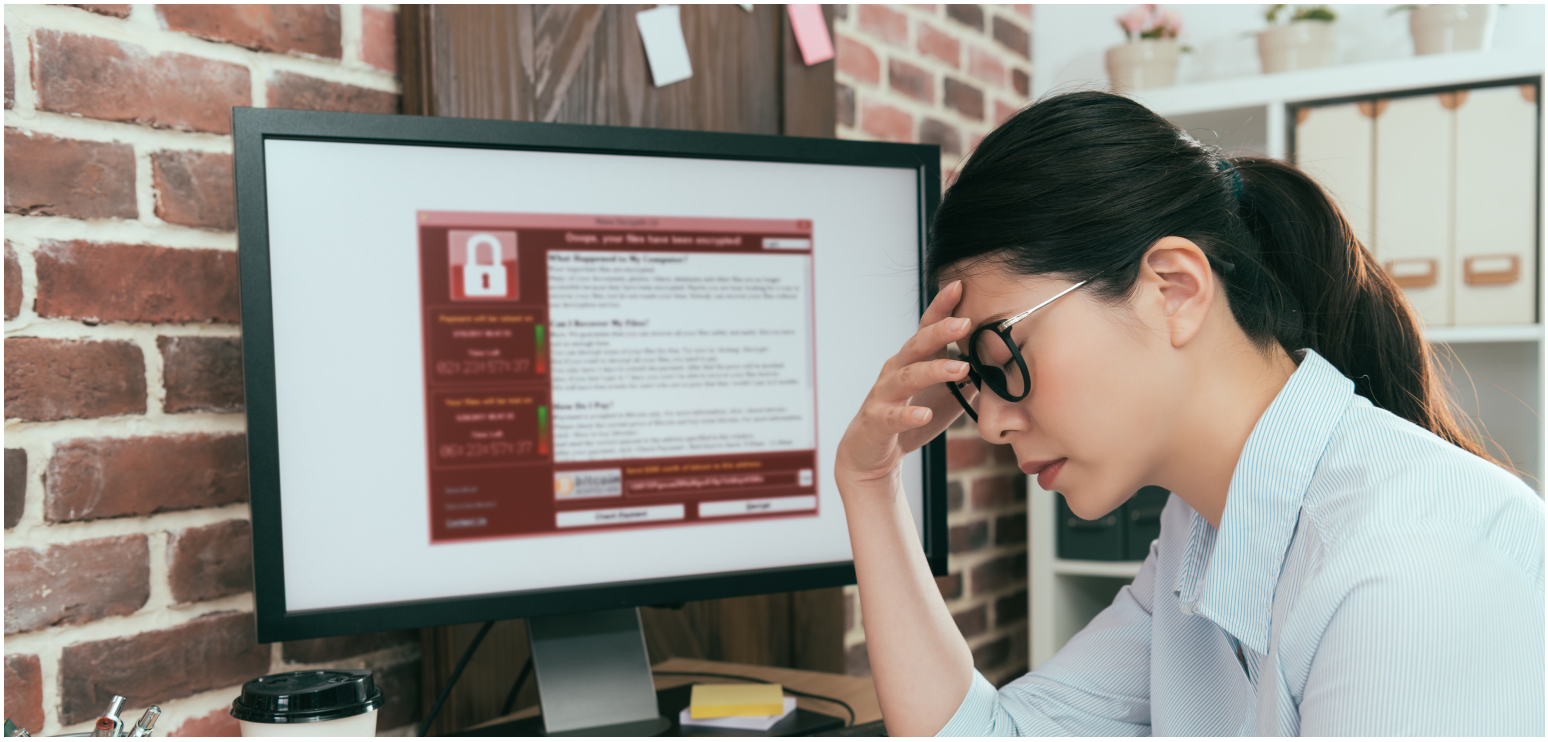
Question 3: How would you know if a hacker had access to your network right now?

Many of your customers and prospects operate under the false sense of security that since they have a variety of common cybersecurity controls (f*irewalls, Anti-Virus software, strong passwords, etc..)* deployed that they are protected from hackers. In reality we know that hackers compromise these controls and gain access to private networks regularly.

There are typically two ways your customer learns that a hacker has compromised protective defenses and gained access to their private network.

1. They are notified by an employee whos machine or data is suddenly unavailable, deleted or encrypted... or
2. They are notified by detection tools and software that there is abnormal activity or traffic patterns that indicate a potential attack.

Discuss these two circumstances with your customer and encourage them to invest in detection tools such as IDS/IPS and SOC services so that they have the capability to know when their cybersecurity controls have been compromised and can stop an attack before the damage is done.



Question 4: Can you trust your employees not to accidently download a computer virus?

Believe or not, the most common response to this question is, "Yes, yes I can trust my employees to not download a computer virus." From time to time you will get the honest answer of, "No, I cannot trust them."

If the answer is YES then you have an opportunity to talk about how common and effective phishing attacks are and find out just how this customer believes they are immune to them. Have they ever tested their employees? Are they provided regular security awareness training? How do they defend against this incredibly effective attack?

If the answer is NO then you have any opportunity to discuss the benefits of having a comprehensive cybersecurity awareness training program. Show them the training content and talk about the advantages of transforming unsuspecting, naïve employees into informed and responsible cybersecurity stewards!

Question 5: Who is responsible for the oversight and execution of your Cybersecurity Program?

Countless cybersecurity regulations demand that someone is assigned ownership and responsibility for an organizations cybersecurity program. It makes sense, if no one is responsible for cybersecurity, then what will the outcome be? Imagine if there was no one responsible for finance and accounting? Would the financial statements be reported in a timely and accurate fashion? Effective cybersecurity requires the same level of ownership that other critical business functions are assigned.

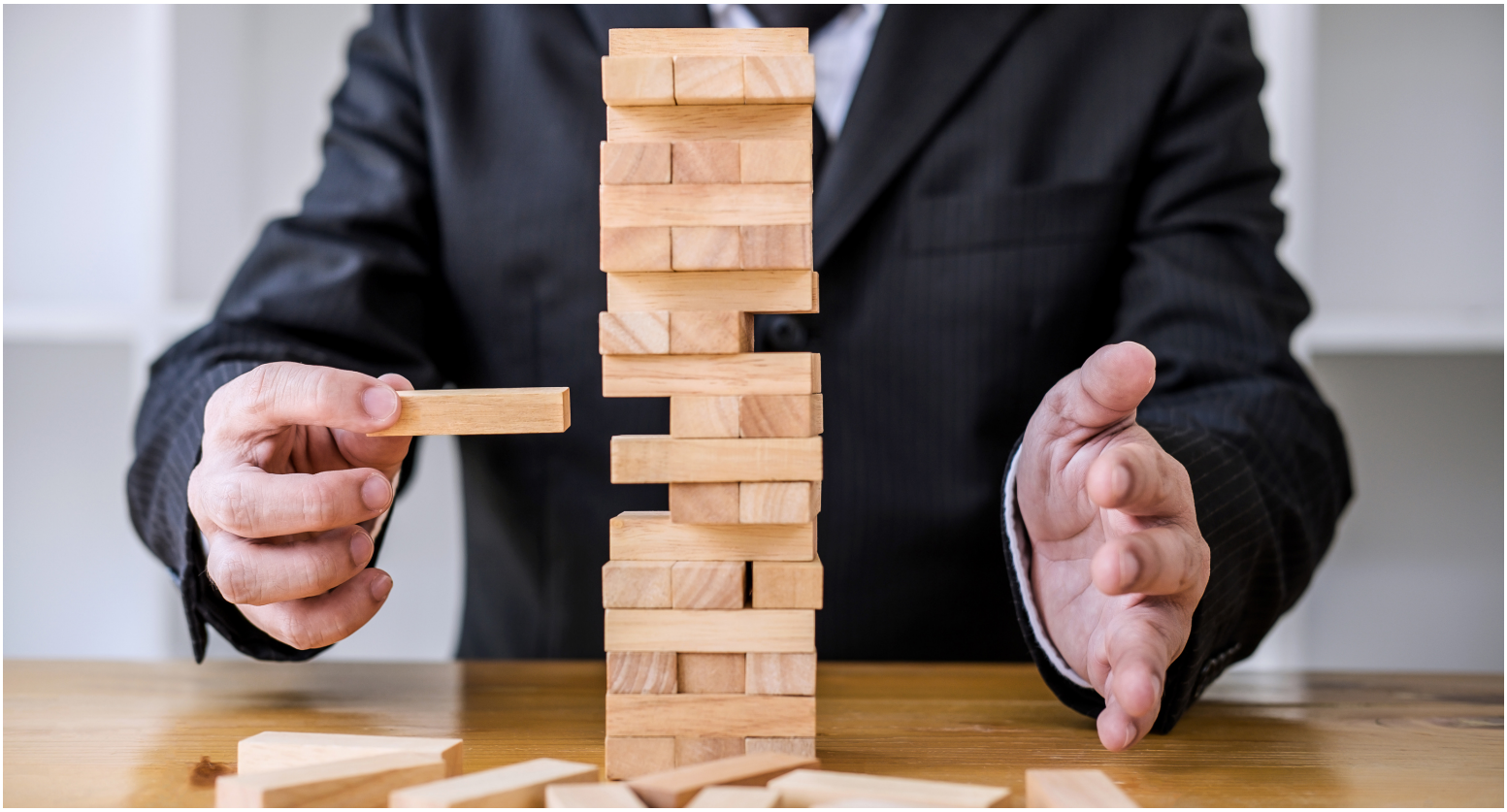
And what is a "Cybersecurity Program" anyways? It is a documented strategy and plan designed to protect the organization from cyber threats and vulnerabilities and reduce overall risk.

Your customer may not have a cybersecurity program and they may not have anyone responsible for creating and executing it. You can offer them help in a BIG way and become that critical resource.

Question 6: Do you think that hackers are targeting your business?

If the answer is YES then dive into a conversation about what your customer is doing to address this dangerous threat. Ask them about the content of their cybersecurity program, their protective controls and their overall ability to detect, respond and recover from a cyber attack. There will be a chance to help them get better in some way!

If the answer is NO then you now have an opportunity to educate your customer or prospect about the actual demographics of businesses that fall victim to a cyber attack. Hackers are opportunistic. They are targeting organizations that lack sophisticated defenses. Many people believe that hackers are only after the Fortune 100 firms - but the truth is that most attacks are executed against small and medium businesses. Show your customer that they are THE target and then offer them the solutions they need to protect themselves!



Question 7: What is your greatest risk associated with cyber threats?

This question is deigned uncover just how mature your customers' Risk Management program is - or - if it even exists at all.

If they do not know what their greatest risk is then how can they properly allocate resources (time, money, and human capital) to protect themselves from cyber threats?

Offer to complete a Risk Assessment for them. It will explore adversarial, accidental, technical and environmental risk events that are unique to your customers' business operations, technology environment, critical assets, sensitive data and exposure created from threats and vulnerabilities. You have the power to not only identify the greatest risk(s) for your client, but to then craft amazing responses and solutions that mitigate, transfer, eliminate or reduce that risk. Now that is real value.

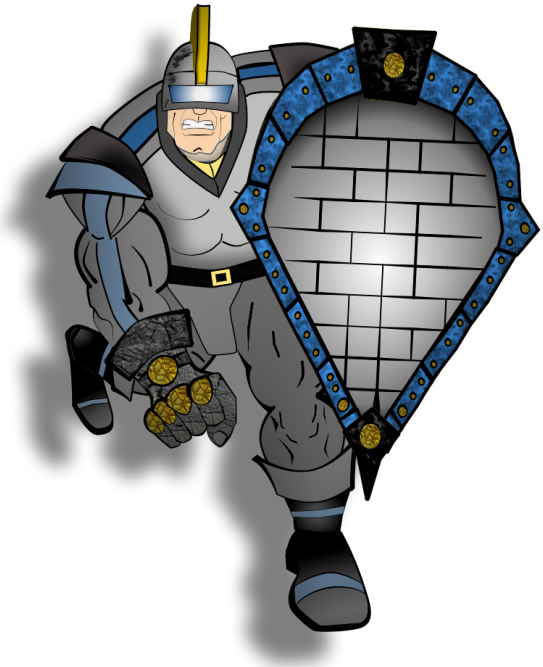
Question 8: Can you explain to me how you protect yourself from hackers?

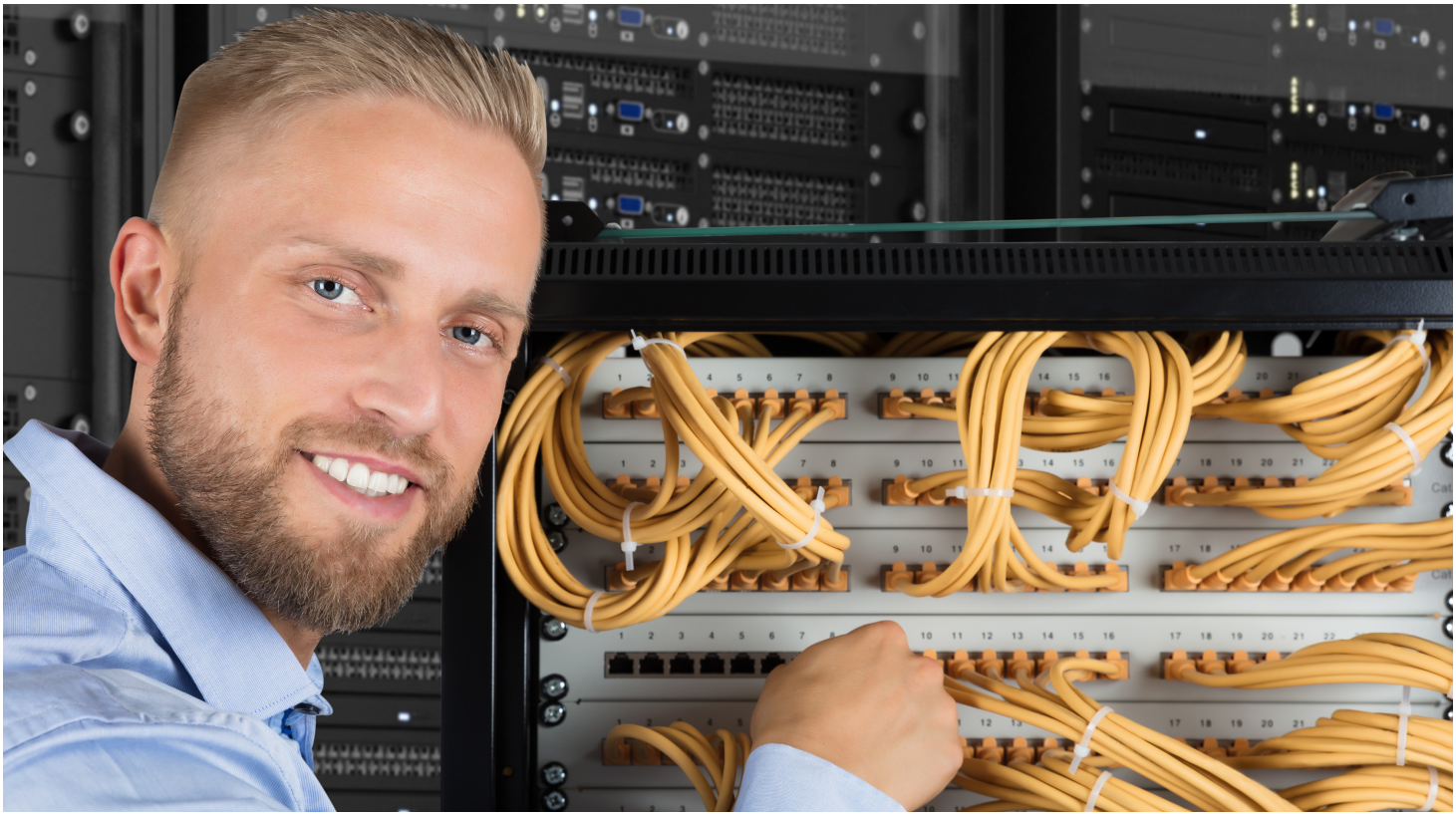
Most of the time the response to this question will come in the form of a list of cybersecurity controls. For example, " We protect ourselves by having a firewall, email encryption, web content filtering, and multi factor authentication."

Ok... now you have to ask two additional questions:

1. How do you know those protective controls are working? Have you tested them?
2. How do you know those protective controls address your unique risks?

The objective is to encourage your customers to regularly undergo Penetration Testing to ensure their defenses are working - and - to make sure their defenses are addressing their risks by perfomring a Risk Assessment.





Question 9: As your MSP, do you hold me responsible for your cybersecurity?

This question has a funny way of opening a conversation up about what you, the MSP, is contractually responsible for and what you are not contractually committed to provide - despite what your customer may assume.

You may provide helpdesk services, infrastructure support, proactive maintenance, advisory services, and perhaps even manage several security controls like firewalls and endpoint security solutions.

Chances are you are NOT committed to provide vulnerability management, risk management, policy development, and penetration testing. You probably are NOT creating and executing a cybersecurity program either! But you can, and you should.

Think abut it... if your customer gets hacked tomorrow, who will they hold accountable? If the answer is YOU, then you should ask to deliver a comprehensive cybersecurity prgram and get paid to be responsible for it!