FTC SAFEGUARDS WILL IMPACT ALL YOUR CLIENTS: What you need to know.

Your clients are on ground zero and a bomb is scheduled to detonate on June 9.

Are you ready?

On June 9 the new FTC Safeguards take effect and hundreds of businesses will be impacted.

QUESTIONS YOU SHOULD BE ASKING YOURSELF

Before this happens, you need to be ready:

- How can you use this requirement to drive security and managed services sales?
- How can you use these new rules to sell security to clients and prospects *even if they aren't covered by the FTC*?
- And finally, how can you make sure you have an offering that will keep your clients from looking somewhere else for guidance on FTC Safeguards oversight?

BACKGROUND

The FTC was formed in response to the Great Depression to prevent another Earth-shattering stock market crash. Between then and now, we split the atom, went to the moon, and created the internet. In our modern world, there are more data security risks than were ever imagined even 20 years ago when Congress passed the Gramm Leach Biley Act based on 1999 technology. (Do you remember what that was like? Back then most people didn't even use anti-virus.) These new FTC Safeguards are redefining who needs to take data security seriously and what rules of the road are needed to protect that data.

Thanks to these updates, many businesses that were previously excluded are now impacted by these new FTC Safeguards, including many MSP clients in the SMB marketplace.

THE vCSO SOLUTION

One of the requirements of FTC Safeguards is having a "qualified individual" who will be overseeing their security program. This is your opportunity to introduce clients to a vCSO offering.

The vCSO solution means that you take the lead in your clients' cybersecurity. You've already invested in them, and you've built up their trust working with them in the past. That puts you in a prime position to lead their cybersecurity at a time when they need someone.

Right now, there is an extreme shortage of leadership in cybersecurity. Too few experts are available to fill positions, and even those who are calling themselves experts are often fresh out of college with little to no real-world experience. Companies are so desperately looking for talent that they are hiring people they otherwise wouldn't consider. And the need is getting more urgent every day.

Business leaders today are faced with a scary sight:

- Cyber liability claims being denied
- Businesses on the hook for huge recovery bills
- The risks of falling victim to business-shuttering ransomware attacks or data breaches with virtually no guidance for preventing them

They're looking for help. But help is nowhere to be found. Who should they trust?

YOU.

Think about it:

- You know how their network (or networks like theirs) runs
- You know what their users' pains are
- You even know what those users are doing on a daily basis
- You have an acute knowledge of how SMB networks run

BUT WAIT. WHAT ABOUT QUALIFICATIONS?

Stop telling yourself, "I'm not qualified for this position" or "We could never do this."

Right now, MSPs just like yours are starting to offer this vCSO program to their clients. They are living proof that:

1. All sorts of companies, large and small, are looking for vCSO guidance
2. You don't need letters behind your name to be a vCSO solution

Simply go to **https://www.galacticscan.com/cso-beta** and fill out the form so we can send you an invitation to the Galactic vCSO program.

YOU ARE QUALIFIED

Here's why:

- **You have the experience** — You are FAR more qualified than a 9-5 CSO. You've probably worked with a lot of different companies and have solved a lot of different issues. I am 100% sure you will be a better leader as vCSO than most options your clients have. NOW is your time to make sure your clients are secure and meeting FTC Safeguards.

MY CLIENTS DON'T HAVE COMPLIANCE NEEDS

That's not necessarily true. The new FTC Safeguards have redefined who needs to be covered so there are lots of new businesses who need to follow the FTC's rules. Some of those newly covered entities include mortgage lenders, mortgage brokers, payday lenders, finance companies, and account servicers just to name a few.

ONLY ONE QUESTION FOR YOU: Will you step up and be the person your clients need?

If you want to give away this chance to be a security leader, that's fine. But realize that you will be giving away your relationship as well. Security is about trust. If you are engaged with their leadership and actively planning with the team to address their risks and shore up their processes, you will be their ultimate trusted partner.

If you relinquish this to someone else, they will be in the driver's seat. And do you really want to be sitting in the backseat waiting to see what happens next?

A 9-POINT CHECKLIST FOR YOUR vCSO PROGRAM

We've put together a 9-point checklist to make sure you have the right items in your vCSO program for FTC Safeguards-depended clients and prospects.

The FTC Safeguards Rule outlines 9 separate components required for compliance. Each section listed below is a brief description of the core idea for each element followed by a direct link to the actual standard. Each standard should be read in full before implementation. Remember when reading the standards, your clients are the audience.

- *REQUIREMENT 1: Designate a Qualified Individual*

This "designated qualified individual" will work with the company's leadership and implement the information security program, but per the FTC Safeguards ownership maintains ultimate accountability. This designated person can be an employee, affiliate, or service provider of the client. In most situations, you can insert yourself or someone on your team as this person. You will manage your client's security program and will continue to make recommendations on their security stack. You'll discuss their security risks and guide decisions toward improved security practices.

So, the question is not whether your client will designate someone, because they are required to do it. The question is whether you're ready to be that someone.

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(a)

- *REQUIREMENT 2: Perform and document risk assessment*

Risk assessments are a critical piece to a healthy security program. Until your client understands their security risks and the steps your organization is taking to minimize them, they may be shouldering more risks on their client data than they might expect. This is of particular concern if they have unreasonable expectations with your role as their managed services provider. We suggest that MSPs provide the following to their clients to demonstrate fulfillment of this FTC Safeguards requirement:

1. A written assessment of their security risks. This should be an evaluation you work through with your client, assessing their data assets, policies, and practices.
2. The criteria used for evaluating risks and an assessment system of how the risk assessment was performed.
3. A cadence to additional assessments.

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(b)

- *REQUIREMENT 3: Apply Controls*

Companies will be expected to implement security controls to protect sensitive data. This typically comes in the form of the following:

- Implementing and periodically reviewing access controls
- Deploying encryption for customer data in transit and at rest
- Performing an annual third-party penetration test

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)

- *REQUIREMENT 4: Validate Controls*

Companies will be expected to show that their security controls are working. Third-party security assessments will help identify any controls that are not working the way your team expects. A general rule of thumb is to receive a third-party assessment on a quarterly basis to evaluate their security. We recommend you consider providing the following:

- Evidence of regularly testing and monitoring controls' effectiveness
- Proof that Information systems have been under continuous monitoring or annual penetration testing
- Vulnerability assessments every six months

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(d)

- *REQUIREMENT 5: Develop Training/Auditing Program*

Companies will be expected to provide continuing cybersecurity education to their employees and have an easy way to audit training completion by all team members. Consider:

- Implementing security awareness training and explaining risk assessment findings
- Maintaining sufficient staffing to run the security program
- Verifying that security personnel are staying current on security threats

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(e)

- *REQUIREMENT 6: Monitor Service Providers*

Companies will need to evaluate other vendors that interface or work on their network to make sure those vendors are abiding by their security standards. This entails:

- Engaging service providers that can maintain appropriate safeguards
- Making sure service provider contracts include safeguard implementation
- Periodically assessing their service providers

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(f)

- *REQUIREMENT 7: Develop Continuous Improvement Cadence*

The FTC guidelines require teams to continuously evaluate the state of security. Communication with senior leadership will be required. If there are any concerns, they need to be addressed whether by security tools, changes in processes, or behaviors within the organization. Teams need to evaluate information security programs based on:

- ✓ Testing
- ✓ Material changes in the organization
- ✓ The results of a risk assessment

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(g)

- *REQUIREMENT 8: Document Incident Response Plan*

Your client will be expected to have planned out how they respond to a data breach or cyberattack. Who will do what? How often will they do a mock breach to practice their team's response? You can help them by doing the following:

- ✓ Documenting every incident
- ✓ Providing guidance on how incidents will be addressed, including goals, and processes among several other requirements
- ✓ Reviewing the response plan after every security event

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(h)

- *REQUIREMENT 9: Provide Annual Reporting to Senior Leadership*

Your client will need an annual security readout, which means a complete report of their organization's security: where the problems are, what improvements have been made, and where the program is headed. This would include:

- ✓ An annual report to the leadership provided by their designated qualified individual
- ✓ An overall status of the security program and compliance
- ✓ Material matters related to the information security program (assessments, incident reports, improvement recommendations, etc.)

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(i)

The BOTTOM LINE HERE: The opportunity of the decade is here and if you don't take it, somebody else will.

There are going to be people lined up to tell YOUR clients what's happening, including:

- Their insurance provider. We all know that insurance providers are redirecting their clients from managed security opportunities. This issue has become a revenue killer for MSPs.
- Your clients' clients. If the people and businesses they serve need to comply with FTC Safeguards, your clients will be confronted with challenges. As the effective date nears, you better believe the discussion has already begun.
- Their employees. Specific roles within their organization probably have already heard about FTC Safeguards. Think leadership positions, finance, accounting, or anyone in compliance. These people may be asking questions about what is currently in place OR they may be assuming you are completely covering their compliance already.

OVERWHELMING?

Do you think your clients will be overwhelmed? ABSOLUTELY. That's why they need YOU.

Here's the thing. To be secure and to meet the requirements of the new safeguards, your clients need someone managing their security program and keeping them informed about risks to their business. This goes way beyond simply having tools, and it goes across the entire organization.

Your clients need a complete security program. For them, it means less headache and more success. For you, it means increasing income without adding a single support ticket.

ACTUAL PROOF

Want proof of this?

- **Example 1: Accounting Firm Went From Basic Security Investment to Full Gamut**

One of our MSP partners convinced an accounting firm previously investing in basic security to go the full gamut with a complete advanced security stack and vCSO engagement.

This accounting firm knew they had FTC Safeguards requirements coming. When the MSP asked if they wanted to set up a time to talk about what FTC Safeguards meant, the firm agreed.

Even though the firm was reluctant to invest in more security services, they wanted to know what it would take to close any gaps with the new requirements.

A very successful meeting all started with a conversation about risks, the Galactic risk assessment, and gaps in security. The MSP owner got the firm to agree to a third-party penetration test to see if there were any gaps. A few clicks and 20 minutes later the assessment was done.

The MSP owner educated the client about third-party assessments and how several areas of concern on the third-party report were directly linked to the new FTC requirements. He then showed the firm how the Safeguards would address findings in the penetration test AND that these requirements were needed going forward.

This MSP ended up closing a COMPLETE advanced security stack AND vCSO engagement, amounting to over $10K in new MRR.

The Takeaway

If you have a client who isn't investing in your advanced security stack, FTC Safeguards is a good way to do so.

- **Example 2: MSP Closed $28K MRR vCSO Engagement Simply By Demonstrating Risks And FTC Safeguards Gaps**

Another one of our MSP partners was providing FTC Safeguards for an auto dealership. The dealership was previously paying a different MSP for security services — less than half the price of the current $28K engagement.

The dealership's previous MSP provided a very inexpensive MDR solution. They also provided a software-as-a-service policy management platform. It became immediately clear to the dealership that budget friendly was not going to work for them.

Our partner offered a third-party evaluation of the dealership's security. The partner performed a penetration test for the dealership of their environment.

The MSP then showed the dealership a report of all the things that were not working. The dealership ended up getting really upset because they thought their MSP (at the time) was doing everything. The

MSP was not doing everything because the most basic services do not provide compliance as an offering. When your clients find out, this really pisses them off. This partner was able to sell them a $28K MRR deal of just vCSO services and his advanced security stack. This added ZERO support tickets and labor for his MSP team.

The Takeaway

A significant number of business leaders mistakenly believe they have security handled because of some software or an inexpensive, corner-cutting security stack. But the truth of the matter is that won't work.

If you aren't communicating with your clients about their compliance requirements and putting them into a risk-based framework, they will be assuming you are doing everything for them. If you aren't charging them for additional compliance work and are just handing it off to a cheap software-as-a-service solution, you may not be doing enough. This dealership in the above example decided to "kick the tires" and test out the solutions that their previous MSP had been offering. The third-party report revealed so much risk and liability that they decided to switch solutions, doubling their security spending within hours of the meeting.

This client was a budget-conscious penny-pinching, do-not-want-to-invest in security if it's not needed, client. Think of your client base and how many clients fall into this category. They may assume you are covering their compliance work as part of their service agreement. If you aren't communicating their risks AND showing them a solution to address this stuff, you will eventually have upset clients trying to get out of their contracts.

vCSO GUIDES THEIR COMPLIANCE

That scenario is terrifying, isn't it? If you are a vCSO though, this example shouldn't happen to you because you would have a way to guide your client's compliance.

These vCSO positions are in HIGH DEMAND right now. The SMB marketplace is experiencing an extremely short supply of qualified CSOs right now. Colleges churning out an inexperienced workforce are farming out their novice candidates as soon as graduation day. This is an unprecedented demand for all talent.

But you have that talent within your ranks. With your experience across a diverse array of networks and the gamut of computer problems, you and your team are qualified to fill the skills gap in cybersecurity leadership today.

READY TO KICKSTART YOUR PROGRAM?

To receive an invitation to the Galactic vCSO program, go to **https://www.galacticscan.com/cso-beta** and fill in your email address.

Need more information on how to kickstart your program?

Visit **www.galacticscan.com/vcso-kickstart** for a complete video of how this process works.