# #187 - Ensuring Profitable Growth

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G. Mark Hardy. I'm your host for today, and we're going to talk about how CISOs can help ensure profitable growth of a company's products and services.

Now, that's a little bit of a different concept than we're used to because We're always told that security is a cost center, and like toilet paper, you spend the least amount of money to make sure you've got something there and you're compliant, but usually the pursuit of financial excellence and security is difficult because you're competing against other parts of the organization that generate revenue.

Today, I'm going to give you some concepts as to how you [00:01:00] can rethink that particular mental model and perhaps re educate your executives through your behavior and show them that you can indeed help improve profitability as your CISO or security leader. So if that sounds interesting, let's listen in.

Now, first of all, we're talking about growth and the idea of profitable growth. Now, the reasons that most companies exist is to ultimately make a profit. Although, if I recall from my MBA class in marketing, the purpose of a company is to attract and retain customers. Think about that. In any case, the reason that we want to make a profit is that in failure to make more money than you spend eventually will cause the business to go out of business.

That was a lesson that we learned the hard way back in Y2K, when just before that with the dot com boom, all these companies were saying, well, we don't have a solid business plan, but we got a lot of customers, we lose money on every customer, but we're going to make it up on volume. [00:02:00] In any case, there are exceptions like non profits, government sector.

They don't focus on making a profit, but majority of people in the world who work for companies are going to focus on earning a profit. Now, what is a profit? You might say, well, it's income over expenses or the surplus of cash left over or what evil capitalists go after. My definition that I came up with in B school a long time ago was profit is the result of predicting the future more accurately than others and then acting upon it.

And I had to add that last part of it because I look at the world and I see an awful lot of things over the years. You can see what's coming next and you can potentially make a lot of money off of it, but it doesn't have to be money. You can have a profitable relationship emotionally by marrying the right person, or a profitable emotional relationship and just feel good with your friends and your team and things like that.

So think about it beyond [00:03:00] just money, but here we're going to focus more about something tangible and the money. I'm going to suggest there are four primary business objectives that enable a company to increase its profitability. And therefore, if you can improve on those business objectives. You can have an impact on the bottom line, which will reflect well upon you and your career, and hopefully your next request for security resources.

Number one, companies perform customer and market outreach. Essentially, if the company finds new customers who buy things, that means more money to the company. If you sell the same product to a hundred customers, then you should make, theoretically, ten times more money than just selling to ten customers.

Of course, there's fixed costs and variable costs, but let's not get into the details for now. If your company is focused on this through sales and marketing efforts, then you should find ways to enable the sales and marketing efforts to improve. And this means improving, often, the customer experience.

Now let's [00:04:00] look at this from a customer perspective. Imagine a customer wants to obtain a new car. So they can go to work, and pick up groceries, and drive around the neighborhood, etc. The customer has to consider the options of renting, Getting a used vehicle or getting a new vehicle. Usually that means the customer is going to browse websites to look at pictures, specifications, and reviews of cars.

So the goal of this type of business is to create a top tier experience where a customer can find the information that they want to see. They might even request a quote on a car with various options. Your company's website should show the manufacturer's suggested retail price, the MSRP, initially. Now, of course, most dealers can go below that, and often will, unless it's a hot vehicle, and then everybody wants it, and then they go above.

But your website might also ask the customer if they want to be connected with a local dealer for a custom quote. Now let's think, how could cyber better enable this experience for the customer? The business has high [00:05:00] expectations that these websites are available and provide a seamless experience for the customer to find what they want without having to go through multiple clicks.

They're not trying to create a friction, difficult, Cavity search on your website looking for stuff you want a safe, secure, frictionless experience. It goes smoothly. Consider how cyber can support that goal for the customer. Think about it. Once the customer decides to make a purchase, they're going to register in a customer portal.

They're likely to have to sign some agreement to be contacted in case there's a product recall. The customer may consent to receiving communications from the marketing team if they want discounts on upcoming services. Customers may also purchase some insurance or extended protection plans or warranties to protect their car and its parts over the life of the vehicle.

Now here, cyber plays an important role in protecting customer information. Should have a site with MFA, multi factor authentication. An absolute minimum these days MFA [00:06:00] in 2024 is like passwords maybe in 1980. You wouldn't want to have a system without it. But in addition to MFA, encryption, something that will block bots from flooding our sales team with worthless leads, might also implement data loss protection or DLP technologies that ensure that we don't send it back to the customer their sensitive data by email.

You could champion a website portal where customers can talk and help desk agents on our web platform can assist them. And if our DLP works as intended, although the customer was able to securely enter or upload PII, were their own email a compromise later? Well, guess what? That sensitive information wouldn't be there in a confirming your email from you.

Naturally, you have to protect your own IT systems, but by doing something like this, you're limiting the blast radius of any breach of compromise by compartmentalizing that sensitive information. Another example of improving the [00:07:00] customer experience is using a solution like DocuSign or some similar type of online Signature capture.

In 2024, no one should have to fill out a paper form with a black pen, scan it, unless there's a law requiring it to be performed that way, and in some cases there are. It inconveniences the customer to find a printer, actually have a printer, have some ink that'll go with it, make sure you're full of cyan, even if it's black and white, you know, get the, get the joke, you know.

Sign. The printed document, but first you have to get it off the web to get there, then you fill it out, you sign it, you scan the document, upload it back to the company. 5, 10, 15 minute experience at best, if everything's right where it needs to be. However, if the company can put all this into something like a DocuSign, the process can be 30 second experience with all these steps.

Log in, By clicking the link, initial, initial, apply signature, click submit. Wow, that was easy. Plus, by adding MFA into [00:08:00] the DocuSign or equivalent login, you can ensure the customer is who they say they are. You can verify a known value such as their phone number. Rather simple MFA, but often works. It is not going to stop 100 percent of the fraudsters, but it will stop many.

And the user doesn't end up with sensitive information on paper, which is subject to dumpster diving at some future time. Now, once a customer owns a product, your company may want to send maintenance alerts and reminders to get the customer to come in and service their vehicle. You might be doing new things that catch the customer's attention.

Let's say you have a mobile app that provides a notification saying, Um, It's been six months since your last oil change. Here's a 15 percent off coupon that you can apply if you book an appointment in the next seven days. Call to action. Probably going to drive sales to your dealers versus a customer if it just goes to some oil change place outside of your dealer network.

So think about the ways that you can provide these notifications in a secure fashion. The second business objective that allows companies to increase their profitability is through service enablement. Think of it this [00:09:00] way. If your customer only buys one of the parts and services sold, then you're only gonna make a certain amount of money from that customer.

However, if you get the customer to buy more parts and more services from your company, then you're gonna make more money over the long haul. So it's generally in a company's best interest to offer multiple or recurring services to a customer. Remember, would you like fries with that? Think of most fast food restaurants.

They don't just sell hamburgers. They'll sell or upsell fries, soft drinks, and more. Oh, don't forget about a dessert. Make a shake or an ice cream to top it off. The same objective can be achieved in selling cars. Think about it. The markup on parts is often higher than on the vehicle itself. Remember, Honda has to compete with Ford and Toyota and every other manufacturer, so they're going to be uber competitive to keep the initial price of the vehicle low enough to get the deal.

However, once the customer buys into that ecosystem, they really can't buy a Toyota air filter for a Honda Accord, since the size and fit are likely to be different. Car manufacturers sell air [00:10:00] filters at a price that has a much higher profit margin than the original car and in addition, manufacturers look for ways in their contracts to say that if your car is under warranty by Honda, then you have to service it with only Honda parts if you want the warranty to remain intact.

Not great for the customer, but it's great for Honda. And if you buy one of those cars, but don't like it, well, go buy some Honda stock and earn back some of your expenses and dividend payments. With each service that gets created, there's usually a website or a mobile app that customers use to track their item.

For example, email alerts might tell customers what maintenance their car needs. There might be a mobile app that allows the customer to see the telemetry of their car, such as oil pressure, temperature, battery life, tire air pressure. The app might even give alerts saying, Hey, you need to replace or refill something.

And each of those websites or mobile apps can have vulnerabilities. So, Cyber needs to support the business by doing a risk assessment to find out what the vulnerabilities are in each of these systems. You don't want somebody looking up another [00:11:00] customer's data because of an insecure direct object reference issue that allows them to change the customer ID and the URL of a website and start finding other customer data.

Forced browsing type of stuff. Now, do things like scan the code or on the servers for vulnerabilities. Perform threat modeling exercises. Have a pen testing firm come and try to breach those applications. Thank you. Enroll your app in a bug bounty program or something else. Find ways a bad actor could abuse your system to defraud your company and your customers.

And if you can secure those abuse cases, then you can help the business owner sleep better at night. Knowing their systems are protected. The third business objective that allow companies to increase their profitability is continued profit generation. You can often think about this as margin and volume.

If your company sells a car for 30, 000 and has a 30 percent profit margin, then your company makes 9, 000 per car. If you want to make more money from a sales [00:12:00] perspective, then you have to do either one of two things. Sell more cars or increase the profit margin per car. As a cyber organization, you don't really control either of those things.

That usually goes to the sales team. What you do control and influence is the operational resilience requirements. For example, if 80 percent of the sales of the company come in from two websites, making sure those two websites don't go down is probably one of the most important things you can do. You can perform disaster recovery exercises that say, if this system had a bad production change, how fast could we redeploy the previous working infrastructure?

Additionally, you could work with the business to create business continuity planning and testing exercises. For example, if your company had a ransomware event and the website went down, could you take orders via fax, a different website, or some other method? So your business doesn't lose profitability if it takes 21 days for the ransomware event to end.

Now, beepity, beepity, beepity, breaking news. CDK Global, whose [00:13:00] software services over 15, 000 auto dealers in the United States, had to shut down all its systems on Wednesday, the 19th of June, disabling auto sales across the country. Many of these dealers didn't have a backup plan. They couldn't take orders.

So don't forget about defending against supply chain attacks. Just because there's an app for that doesn't mean that you've got resilience. Now having effective tabletops that show response plans, formal communications with customers and how systems would be restored and how critical decisions can be made can really help with the operational resilience for any organization to survive a crisis in the best possible way.

The fourth business objective for companies to increase their profitability is to cut costs. If we can increase our profit margin from 30 percent per car to 40 percent per car, then obviously we make more money on each car sold. Organizations will perform cost reduction exercises like cutting headcount, reducing training and travel, marginalizing R&D functions, and other things they view as discretionary activities.

The [00:14:00] problem is some of those are a little bit short sighted. CISO, you want to find ways to help the organization perform that function And consider recommendations, but not creating technology debt, not creating a situation where like deferring maintenance, you can skip an oil change on your car this month, but you skip it for too many months.

You're going to seize up that engine. So what you want to think of ways to do that is how do we improve our efficiency, our effectiveness so that we can reduce the costs and not have to go ahead and do crazy things like cutting headcount or, Suspending all the training for our people. Let's start taking a look first at, well, time cards.

Imagine that if you had the time sheets, the cards, that tell how many hours each developer spent on new features versus operations in support of their application. You might find applications where 40 percent of the time is spent on new features and 60 percent on maintaining the app and just keeping it going.

Let's say one of those application teams has 10 developers. And if you add up the [00:15:00] cost of salary, and benefits, and healthcare, and all the other overhead, maybe it's going to cost you 250, 000 a person. That total cost of that app, just for labor, is 2. 5 million every year. If 60 percent of those costs go to maintenance, that means 1.

5 million is being spent annually. On maintenance, that seems like a lot of money. It's already written! But what if you could replace that system with a serverless solution that only has a 20 percent maintenance overhead instead of 60%? That means you could save 1 million every year in future labor costs.

If the anticipated costs of a rewrite were 1. 5 million to get there, that means within 18 months, you're already cash flow positive on the deal. You've met your ROI. That's pretty quick. And it's smart action to take now, because it's lowering your technology debt. It went away when we built that application to be serverless, but just add a few security enhancements into the product that [00:16:00] make it even better than before.

And now we have a solution that works for everyone. Developers get to tell their management they're building a next generation solution that minimizes their time waste. Chief Financial Officer has a way to show they're reducing costs by using headcount more efficiently to build new features and benefits.

That business always wanted, and cyber gets to make the claim that we're getting more secure. So finding ways to reduce technology debt is a great way to make friends with the business and improve the profitability of the company. Another example of this is looking at inefficiencies. Let's say your third party risk management team asks vendors to provide a Cloud Security Alliance Consensus Assessment Initiative Questionnaire, or a CAIQ, which is pronounced "Cake".

Piece of cake, right? These questionnaires, however, have over 200 types of questions usually, and then your organization will ask the vendor to say, Hey, can you give us a SOC 2 Type 2? And while you're at it, how about an ISO 27001? Now, if your team reviews all these documents, you're doing redundant work.

Because there's a lot of overlap between a [00:17:00] SOC 2, ISO 27001, and the CAIQ. You might want to find if the vendor completed the ISO 27001, and if so, maybe you reduce the questions that you ask By 80 or 90 questions, they're already answered. It saves your vendors time when responding, saves your risk and compliance specialists time when they review the submissions.

And as somebody who's had to fill out a number of these things as a CISO, I've got to tell you, I'd feel a whole lot happier working with a company that says, Hey, wait, you already told us a bunch of these things. We're just going to ask you the things at the margin. Now, that's just a simple example, but there's a lot of inefficient activities that we all do in organizations.

Ask your coworkers. Where do we find low value work? What's tedium? What is it that has to get done but doesn't add a lot of value? Where could time be saved? Do we really need to fill out a CAIQ or a SIG filled out if the vendor has a SOC 2 Type 2 attestation or an ISO 27001 certification? If you think it does, maybe ask the next question.

If you were to look at the top 10 or even [00:18:00] 20 major breaches from last year and their root causes, how many of those would have been flagged by a CAIQ or a SIG questionnaire? You might find the answer is zero. And if that's the case, you should consider this activity more like a compliance exercise. And if you do just enough to keep the auditors and regulators happy, but no more so, why?

Cause then you can use the resources that would have been spent on compliance, working on things that actually stop attacks against your company. Hmm. Okay. Let's recap. CISOs can enable profitable growth. And you do that by one, improving the customer experience to enable customer and market outreach. 2.

Performing vulnerability management and risk assessment activities on critical services. 3. Enhancing operational resilience on the core services that create the largest company profits. And 4. Lowering the technology debt to enable cost reduction activities. What do you think about that? Yeah, you can do [00:19:00] things like that.

So make it happen and add value to your organizations. So thanks again for listening to CISO Tradecraft. We appreciate you being committed to becoming better cybersecurity leaders. Now, one of the things I'm going to be excited to share with you is we're doing something really cool. For the last four years, just about, we've been primarily sharing our content on this podcast.

We've been asked more than once if we could put together a CISO training course that Perhaps isn't as expensive as the SANS Institute or the cost of getting a university degree or even a certification. We want to let you know that we've heard you and we're now building a CISO training class that will help you take your CISO skills to the next level.

If you're interested in taking a training class from us at CISO Tradecraft, drop us a comment up at the top at CISOTradecraft. com or reach out to me on LinkedIn. We'll be willing to share with you a little bit more about what we're building and get your input on that too. Cause we think it's something you're going to love and the tools and techniques we're going to share with you in the course are going to be something that will instantly help you as a CISO improve your tradecraft.

So please go to [00:20:00] CISOTradecraft. com or our LinkedIn page. Drop us a comment or feedback or a private note. That's something that would interest you. Well, thanks again for listening to CISO Tradecraft. We hope that this has been great for you. I'm your host, G Mark Hardy, and until next time, stay safe out there.