#225 - The Full Irish

[00:00:00] **G Mark Hardy:** Hey, we all like stuff from Ireland, right? We had St. Patty's Day, maybe even had green beer. I've got something even better for you. It comes from the Ireland's National Cybersecurity Center. Stick around. I'm gonna tell you all about it.

Hello, and welcome to another episode of CSO 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, and today we're gonna be talking about what I call the full Irish. We're gonna take a look at a useful government reference, but it's not from the US government. This time I'm referring to the 12 steps to cybersecurity. Guidance on cybersecurity for Irish business, which is published by Ireland's National Cybersecurity Center.

Now, if you're not doing business in Ireland, you don't have to stop the re-play. Why? Because it's got useful stuff for pretty much everyone. Now, [00:01:00] you can access this document today at ncsc.gov.ie. We'll put that link also in the show notes, and it has a structured framework. To help enhance your cyber resilience, and one which you can use to either build a program from scratch or improve your existing framework by identifying missing components and then filling them in.

So we're gonna begin with an overview of the document. Look at each of the 12 steps with some details that get you thinking about how you're implementing these ideas and how you might wanna approach them if they're missing. But first of all, why am I talking about. Ireland number one is because I think a lot of US companies have set up shop in Dublin because they enjoy a rather favorable tax rate of 12.5%.

some examples IBM had its first European headquarters in Ireland. I. In 1956 and still a major employer over there, Google has a large presence in Ireland. Operations in Dublin, apple over large campus in Cork, Microsoft, huge operation center. [00:02:00] Meta. What used to be Facebook is in. Dublin as well as Adobe and Twitter, which is now X and TikTok and, Airbnb.

All these offices are there, which have really transformed the east side of Dublin from the Dockyards, which is fairly cheap and shady neighborhood to now. Very expensive if you ever go visit that place. Both with a lot of brand new

buildings, very fancy infrastructure, and of course the residents to hold all these people there.

Now, great that you have a low tax rate, but there's ways that. Companies even avoid a little bit more knowing a little bit on the side, but I've always interesting 'cause we're coming up on tax season, what some organizations do to avoid paying, a lot of tax. And there's a reference I found that talked about the double Irish Dutch sandwich.

I. How's that for a name? It's a tax avoidance scheme that's used by multinational companies. It involves setting up a couple subsidiaries in Ireland, a holding company and an operating company. And the idea is the holding company registers in a tax haven, which means you [00:03:00] don't have to pay taxes on its profits.

The operating company will then transfer its profits to the holding company, and then you're gonna lower your taxes. And then you could send this holding company to like a subsidiary and. Ireland or Holland, or maybe use it to a bank account in The Bahamas where it's effectively tax free. So now you can avoid paying taxes on profits in Ireland, tax the United States.

And if you use things like the Netherlands as a transit point, you could avoid paying taxes, higher taxes than other European countries. Now these are all legal loopholes, just like we talk about cybersecurity. zero days and until somebody patches them, they still work. But there's been a lot of increased scrutiny and an effort.

To go ahead and create a minimum tax rates to avoid all of this money, moving money around. and so the idea is that companies can save a lot. Google, last year I could find data on was 2017. They estimated avoiding $3.7 billion in taxes, which all goes to [00:04:00] profits. Either to the shareholders or to the executives who came up with the idea by using this approach.

apple 2016, again, dated information from my research, avoided $8.5 billion in taxes, and then Facebook, 2018, 15.8 billion not paid. That would've been taxed otherwise. So I could understand that why companies and wanna go there. But there's also a flip side to it, the Irish Data Protection Commission.

It's not all fun and games. Was fined in May of 2023, 1.2 billion Euros, which is the largest GDPR penalty to date. The General Data protection Regulation, which sets up all the requirements for, protecting, people's privacy and information and things like that. they had systemic ongoing data flows that went

past the revoked privacy shield that EU had It was basically [00:05:00] were laws that said yes, you could move stuff of European citizens someplace else. That law got repealed. They kept doing it. Yeah. TikTok, September, 2020 345 million Euros. LinkedIn, Ireland, 310 million Euros in October, 2024. Meta 265 million in November 22.

another one in January of 2023 for 390. and I just have another one for meta that I just downloaded with some December of 2024, 251 million euros. Now that is a spectacular amount of money, but if you figure that if you lose a few hundred million and you gain several billion in tax savings, just the cost of doing business.

So anyway, if you're not in that role where you're setting up multi-billion dollar type of transactions, we're probably more in the realm of saying, we gotta deal with things that perhaps do cross border transactions. So let's take a look at what Ireland suggests that we do. Is there 12 steps of cyber security?

It's gonna [00:06:00] frame risk as a reality. Basically saying it's not a matter of if, but when. We all know that for the most part, but now it allows you to go ahead and focus on the idea of let's go ahead and look at our threats. Understand their risk appetite, be able to react and defend in real time. Now, it does propose an interesting concept, a 12 month activity plan, which fits nicely with having 12 points.

And what you can do is have each one of these in a given month. Now you might say, I've already got these things. Great. However, nothing says you can't go back on a regular basis and improve and take a look at things. So if you had a focus of the month based upon this plan of 12 things. Because remember we talked about more technical controls like the Australian eight, and that's a different episode.

But this is more looking at the management level. It's a tool to align our cybersecurity with their business objectives. And therefore what we can do is as cyber crime continues to grow and evolve and criminal enterprises are doing [00:07:00] their effort to make money, and oh by the way, I'm guessing they're pretty much tax free, this is your chance to go ahead and build better defenses.

So let's take a look at each of them. the first month, if we do January, doing a rolling year, but you can shift it around, or as I said, you might always say, I got this one. But think about setting things up. The first one would be looking at governance and organization. That means senior management has to provide their commitment to what you're doing.

As well as defining clear accountability. You don't need the chief incident scapegoat officer to be the person that everybody blames and said something went wrong. You're in trouble. You're getting fired, or you're getting sued, or whatever. There should be a more robust framework for that, and what we wanna do ideally is ensure that, first of all, we know what our business drivers are, what are the regulatory frameworks that are going to cause us to have to worry about things?

All those fines that I pointed over to, that I just read on that other screen all came from what. Failure to comply with regulation, that is a huge [00:08:00] risk. And although we look at hackers and criminals and disgruntled employees and dishonest, customers taking your money, governments are very happy to take their money too.

And somebody had told me, and I, gotta check out on this, so if you know the answer, give me a note in, in LinkedIn that if you are an EU country and you successfully have a GDPR fine that is credited toward your dues for the eu. So you actually save your country a little bit of money. And so there's actually an interesting incentive there.

Again, I don't like dealing in rumor that was outside my scope of research, but I heard that recently and if that's the true, it's interesting. So anyway, what we're looking at in terms of doing our governance and organization perhaps get a cyber risk management group together. Look at cross-functional representation.

Have your it have legal risk operations, and make sure that you have your policies established. You wanna look at data protection, particularly things like the GDPR or whatever regime you're operating in. How about remote access? [00:09:00] Do you have requirement for multi-factor authentication? Something I strongly believe it.

maybe you have a concern about tracking across different countries and making sure that you're compliant in each of those frameworks or even the United States. We might find that we have a patch of frameworks. So that would be the first thing is working at your governance and organization. What's the next step?

Could be the next month, or we could just go ahead and, follow, identify what matters most. Now you have to know what your assets are to protect them. And you wanna look at your business objectives that generate revenue, that support people, process, technology, and data, and protect those, we wanna then rank them by criticality.

If you've ever gone ahead and look at your BIA, your business impact analysis, that's really what we're talking about here. If you're a healthcare provider, you really care about electronic health record systems. If you're a retailer, you wanna look at your payment [00:10:00] platforms. Whatever your ecosystem happens to be, you're gonna have some primary focus around that.

Then look at your suppliers, look at your partners. Think about how we go ahead and move information back and forth. What about supply chain risk management? Then come up with a technology asset management program. Centralize all this data. Make sure you catalog what you have, that you can understand what is in your environment and you've got some visibility into it.

And that was the beginning and the end of step two. On the third step was understanding the threats. If you think about it, strategic defense requires that you have good threat intel if you have a cyber threat intelligence capability, which is often done through third parties. I tell people, if you're gonna gather threat intel.

Within your environment, you're cool with that. Why? Because attackers expect you to be looking. If you pop 'em, they're gonna yeah, okay, they found us. But if you're doing your own threat intel, going into the dark web and trying to poke around in forum and to pretend to be somebody you're not, [00:11:00] and you get caught, you might get some severe retribution.

So my thought is, let's somebody else take that risk and then pay for that report. Plus they know what they're looking for and they've been doing it for a while, but you wanna understand who your key adversaries are. Whether they're apps, advanced, persistent threats, nation states, ransomware operators, insiders, what are the motivators that are causing this?

And if you understand what they're going after, whether it's financial gain, whether it's competitive espionage, whether it is vengeance or whatever it happens to be, you can then start to figure out what's gonna drive them. If you use a Mitre attack framework, and you have seen a lot of mappings from apps and known threat actors to that.

You know your tactics and techniques and how they're gonna go ahead and attack you. And if you have multiple threat actors and they're using similar tactics and techniques, that common element is gonna allow you to come up with some good defenses that are going to yield really good returns. Why?

Because they're gonna potentially catch more than one adversary. [00:12:00] Be part of industry forums. If you don't have an ISAC or if you have an isac, go ahead and join it. And if you're not, maybe think about getting one going. If there's a whole bunch of them, I am a participant in the financial services, the FS-ISAC, and there's plenty that are out there.

And then share that information. Make sure that you record your information in a risk register where you can then go ahead and keep track of where you think the threats could impact you and keep that up to date. On the fourth step, we then want to go ahead and make sure that we've appropriately defined our risk appetite.

Now what we talk about risk appetite. Somebody like Elon Musk is going to probably have a much higher risk appetite than somebody like a Jamie Diamond. In the banking world, you are not rewarded for taking big chances. You tend to be a lot more conservative, but if you are an innovator and you're trying to get well people to Mars and things up in the air and back down again and do innovative technology, you're willing to go ahead and try [00:13:00] something a little bit more risky.

that risk appetite. Needs to be owned and defined from senior management. The last thing you really want is to hire an employee who says, yeah, let's go ahead and bet the farm. I got Nick Leason. You can go look that guy up there. The rogue trader who collapsed bearings bank because he went ahead and made all these financial bets.

It just didn't work out to Instead of fussing up to it, he made bigger and bigger ones hoping to recover until finally collapsed. A 200 plus year old bank that had been the bank for all Queen Victoria, think about your risk appetite. Make sure it aligns with the board, says they wanna do. Figure out what risks you can reduce, what risks you can go ahead and transfer with insurance.

What risks you wanna just go ahead and accept and say, I'm gonna live with it. And what risk you wanna go ahead and mitigate and do something about. For example, if you're a bank, you're gonna probably prioritize fraud prevention over internal system risks. And [00:14:00] that way you want to make sure that your spending reflects the approach of what do we care about the most so that we can go ahead and protect that effectively.

Step five, we're gonna focus on education awareness. Now we all have education awareness programs. I would think. Stu Sjouwerman when KnowBe4 the next town over. I remember when Stu hired Kevin Mitnick back in,

November of 2011. I went over to visit him a couple months later and I said, hey, I live the next town over.

Why didn't we wanna work with me? He says, Kevin's infamous. it worked out pretty well, and fortunately we've lost Kevin, but. It worked really well for their business. They went public, made several billion dollars on the IPO. They're private again. They're probably gonna come back out again. So there's still a lot of money available in security awareness and education.

That may not be your concern other than the fact that you have to go ahead and convince your management to write the check, but you want your employees, your contractors, your third parties to be able to respond effectively to when bad stuff happens. Phishing [00:15:00] emails. Road Apples a little USB, I'm looking around for one on my desk.

Fortunately they don't have one right here. But, you leave those laying around, hope someone plugs 'em into their laptop and sees what happens. a lot of these things are gonna target key individuals, people who have access to source code or key executives, and try to get them to change stuff. We now find out with deep fakes.

And the ability of AI to go ahead and fabricate things that are totally plausible, that security education awareness has to go beyond just spotting the, phish. It has to be a matter of spotting the deepfake and being able to have the correct challenge, response, and robust systems to do things. Again, token, MFA, having a third.

Factor instead of just two. There's a lot of ways you could improve on that, but also make sure that, staff can be your layer of detection. We've got great technology. There's a lot of tools that are out there, but at the end of the day, you do so much better when your humans are part of that frontline.[00:16:00]

Number six, implement your basic protections. Now, things like secure configurations. why not? And we understand that most vendors have them. You can go look at CIS. Center for Internet Security, they're gonna have secure configurations. You can download patch management. Are you patching? Are you keeping up to date?

How do you go ahead and do your different windows? We're Microsoft, we have Super Patch Tuesday, and you can have a little test one. Then the first, second, third, and stuff like that. There's always the little give and take. Do I implement? A patch right away and risk that maybe it's gonna break a critical

system, but now the bad actors can no longer exploit those identified vulnerabilities.

Or do I wait a few days to make sure that they work in my environment, but we give the attackers a head start. hey, that's where you're getting the big bucks. You have to go ahead and make this decision. Now we want to go ahead and address the weaknesses, figure out what we have in terms of identity [00:17:00] access management, and ultimately enforce least privilege.

This is one of the frustrating things I think sometimes when you set up your environment to say, Hey, I need to be a global administrator. No, Joe, you don't need to be a global administrator, but I wanna be a global administrator. I've been here for 27 years. Don't you trust me? Of course I trust you. But anything that happens with that ID is gonna be attributed to you.

And if somehow that idea is compromised and something bad happens, we're gonna have to let you go or hold you accountable. I don't want that. So you have to have these conversations to go ahead and make sure that you can get this lease privilege. And sometimes it's much of a human is that it's a technical thing, convincing people that they don't need to walk around with all the master keys with them at the same time.

Data encryption at transit and in rest, especially for mobile devices, retailers, point of sale system. Make sure that you don't have skimmers that are installed or be able to inspect for those. Have some baseline of security and go back through and make sure that these basic protections are done effectively and double check for them.[00:18:00]

Step seven is well be able to detect and attack. Identify, protect, detect, respond, recover. If we go through and we take a look at the NIST Cybersecurity framework, detection enables response. You can't respond if you don't detect it. Attackers that go undetected, particularly for some period of time, can get very deep into systems.

They can understand exactly what's going on. Some of the ransomware attacks that have been done, where you have a adversary that has been in there for several weeks or a few months, you can't pretend to be a poor grandmother from Iowa saying, I don't have any money. They say, actually, yes you do. We've looked at all your financial returns.

We know exactly what you can pay. And oh, by the way, some of the things that you'll find out is some of these attackers will say, we're gonna inform the

government. You breach GDPR and you're gonna pay this huge fine unless you want us to just negotiate with you and then at that point we'll go ahead and settle for a whole lot less.

Now you gotta be careful. You don't wanna repeat the error that Joe Sullivan did where you say, Hey, his team said, let's go ahead and take these [00:19:00] attackers, classify them as pen testers, put 'em under an NDA, that was not thought of very well by the court systems. But when you detect an attack. How quickly does it take you to do that?

Are you watching your logs? Do you have a third party software tool? Do you have your own team looking at it? Do you have your SIEM that's ingesting all this information? Are you sending it to your own SOC? Are you outsourcing it to managed security service provider? You want to go ahead and have robust logging and analysis, and you wanna be able to identify as quickly as possible when a bad actor is in your enterprise, so you can go ahead and shut them down as quickly as you can.

Number eight, be prepared to react. If you have preparedness and you're ready to go, it's gonna limit the negative impact that can take place. If you get sucker punched because you did not have your guard up, you're probably gonna get hit a lot more than if you're expecting somebody to go ahead and make a swing at you, you might be able to block it or duck or even swing back.[00:20:00]

Have an incident response team. Have a tested documented plan. Get legal involved, get HR involved, get communications and PR involved because you gotta go ahead and deal with the press shareholders. Third parties all wanna know what's going on, have some scenarios, simulate them, do tabletop exercise. I love building tabletop exercises for clients like a ransomware.

It locks down your manufacturing system. And now you have to go ahead and decide what do we do? Preparation, identification, containment, eradication, recovery, lessons learned. Looking at the incident response plan. I want to contain, before I eradicate. So what am I gonna do? I'm gonna put blocks around there.

Make sure people know what to do in the right order. Know what your regulation requires you to do, know what your reporting requirements are, and then when do you have to notify? And also, if you have these statements already worked out in advance, in the event that something goes wrong, you can just pull out and say, okay, this is a fill in the blank form.

For if we had [00:21:00] a GDPR breach. This is a fill in the blank form. If we have to report to the Secretary of State, get the work done in advance. So now you're gonna go ahead and not have to worry about how do we start with a blank piece of paper? You've already partway there. Obviously you don't want to go ahead and have something go wrong, but the whole idea is preparedness says when we encountering something bad, we're more likely to have a faster and better response. Step nine is to adopt a risk-based approach to resilience. If you're resilient, it's gonna help you recover better. Business continuity plans with recovery timelines, tie those to criticality because core systems might have to come up within minutes or even hours.

Other systems could wait days, maybe even a week or so, and you still keep the organization running. Make sure you're doing backups. Make sure your backups are stored in a way that they cannot be corrupted. If you get, for example, ransomware in your main system and you've got drive shares connecting you, your backup systems, just going to corrupt all of your [00:22:00] backups and things like that.

ideally you'd like to have some sort of a diode where you can have information that goes this way, but it can't be changed once it gets there. If you're a logistics company, think about warehouse systems. It's huge. The last thing you wanna do is impact your supply chain or not be able to get your business done.

Test your plans by going, ensuring that your plans have been tested. You find little things such as, oh they have an emergency diesel generator. Great. It'll kick in automatically. Great. When was the last time you checked the fuel in the emergency diesel generator to A, make sure that there is fuel and B, that it's not got water in the tank.

It's gonna cause some problems and this thing will actually light off as it's supposed to because you've got enough charge on your battery to go ahead and get it going because if it's replacing your electrical and your electrical is down, how are you gonna start it? So there's a whole bunch of things that you find out that you learn when you actually test your plans that you didn't think they might have happened.

Step 10 is to implement additional automated protections. Now, anything that we can automate from a security prevention or [00:23:00] perspective, let's do it. Intrusion prevention systems. Why not? Why wait until an intrusion happens? Go ahead and try to prevent it. Web app firewalls. If your web developers have some errors in their code, or you have Bobby the intern who's written

something, a web app firewall is a really good compensating control for an error that might be in the code.

It'll catch stuff like that. DLP I'm working through with the data loss prevention for one of my clients right now. that's really important. I wanna automate all that. I don't want anybody manually looking at everything that goes past, automate your vulnerability and identity management, and have a centralized IAM identity access management system to streamline your control for a software developer.

DevSecOps. You wanna build security into your lifecycle, and if you take these measures, you align 'em with your risk priorities, fortify yourself against sophisticated threats, optimize your resources. You're probably gonna end up a lot better if something goes wrong. Step 11, [00:24:00] challenge and test regularly.

If you validate things, you can confirm your readiness. How about an annual cyber incident simulation? Do it at the executive level and then do another one. At the tactical level, you wanna test the decision making during a data leak, for example, and red team exercises, you wanna mimic advanced attacks. Do social engineering drills reinforce awareness.

if you're a bank simulate fraud attempt, you're gonna see where the weaknesses are in making sure your defenses hold up. Let me tell you another little trick, which you ought to do when you're doing your tabletop. I do that. Most organizations have somebody who has designated authority to make a decision.

Make sure in your tabletop exercise, that key individual is unreachable, or on an airplane, the wifi goes down. Why? Because you wanna see if they have a fallback plan. I'm sorry. She has to be. She's the only person who making that decision. You can't reach her for six hours. What are you gonna do now?

we don't have a de have a designated alternate. As a naval officer, I tell you that we had a whole chain of command on that ship. If something were to [00:25:00] have happened to the captain, the executive officer would take over. Somebody happened, the xl, one of the department heads takes over and then finally down to the division officers and finally the last semen deuce is left on board, is gonna be in command running it, but you've always got somebody who's gonna take over.

In the event you lose key people. Make sure that same type of decision tree. Is available so that nobody sits around saying, we can't make a decision now and

do that, of course, during the testing so that the consequence of getting it wrong is much less. And then step 12, create a cyber risk management lifecycle.

Think about this program that we've discussed. Identify your gaps. Maybe your detection needs a little bit of scaling. your governance doesn't have good metrics. take a look at your risks on an annual basis. Reassess them. Maybe your threats have shifted. make sure your compliance and your regulations are the same as they were a year ago.

There's constantly an evolving compliance framework out there. Get together with legal. They should be the ones looking at it, but don't wait for them to contact [00:26:00] you. Get on a regular basis, call 'em up every month or two or three. Hey, is there any new frameworks you need to worry about? Any new compliance requirements they have to take care of, get ahead of the problem and then go ahead and look for.

Emerging threats. There's a lot of information that's available out in the news. It's a very volatile time right now, both politically as well as in some parts of the world. Kinetic warfare. if you're doing business in those areas, it's a really kind of good idea to be paying attention to these things.

All right, so what do we've got? We've taken a look at these 12 different steps of cybersecurity, as a sort of a pragmatic guide for how we might want to go ahead and approach our framework. we can go from governance to testing. We're gonna align our cybersecurity with our business imperatives.

And if you don't have such a structure, here's an approach. Again, establish your governance and organization one. Identify what matters most. Two. Understand the threats. Three. Define your risk appetite. Four. [00:27:00] Focus on educational awareness. Five. Implement basic protection. Six. Be able to detect and attack.

Seven. Be prepared to react. Eight. Adopt a risk-based approach to resilience. Nine. Implement additional automated protections. 10. Challenge and test regularly 11. And create a cyber risk management lifecycle. 12. Now what you have is an annual cycle that you can once a month focus on one of these things, tune it, improve it.

It's not gonna be overwhelming, and if your program exists, but it's incomplete, this helps you fill in some of the holes. And now what you're able to do is get ahead of the problem. Because let's face it, cybersecurity's a perpetual endeavor. We're never done. It's not like we said, Hey, we're set. We're good.

Let's go. Everybody take off for a month. It'll work well. This is a, hopefully a very useful guide if you find this valuable. Let us know. We'd always look for feedback. Here at CISO Tradecraft, we're on LinkedIn. We also do a lot more than just podcasts, so if you're not following us on LinkedIn, please do If you're watching us on YouTube, [00:28:00] great. We're of over 40,000 subscribers there and we'd love to go ahead and do that. We haven't yet got to the point where I'm doing a lot of visual stuff. this podcast is, most people I talk to, listen to the podcast. We target this to be 30 to 45 minutes. It's a workout ride into work or just a time in between.

I try to do it so you can play it at 1.5 x or maybe even two x if you're so inclined. Let us know how we're meeting your requirements to help you on your cybersecurity journey. 'cause that's what we're here for, and this is what we do this for. So thank you for your time and attention. I hope you've enjoyed today's episode about the full Irish, and, this is your host, g Mark Hardy.

Until next time, thank you from CISO Tradecraft and stay safe out there.