Welcome to the CISO Tradecraft podcast episode where we're diving into the world of cybersecurity for enterprises. If you're part of a business you will hear folks asking these three crucial questions:

- Which protections should we start with?
- What tools are needed to implement those protections?
- How much will it cost to implement them?

If that catches your attention, then you're in the right place. We're going to shed some light on these crucial questions.

Commercial Break

First, let's talk about a trusted framework called the CIS Critical Security Controls. It's one of the most accepted standards used in the Cyber Security Industry along side things like NIST CSF or ISO 27001. The current list shows a set of 18 safeguards that enterprises use to defend against cyber threats. Note it used to be 20. For example: The top 5 controls are:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management

Now within the 18 CIS Critical Security Controls there's something called Implementation Groups. There's 3 of them. Implementation Group 1 has 56 safeguards and is designed to represent a minimum standard of information security for all enterprises. Implementation Group Two has 130 total safeguards. Finally Implementation Group 3 has a total of 153 safeguards and is designed to secure sensitive and confidential data and lessen the impact of sophisticated attacks. You can think of this like NIST 800-171 is Implementation Group 1 vs NIST 800-53 is like Implementation Group 2 and 3

Essentially CIS understands that small companies don't have the same level of resources to apply all of the safeguards that a large company would have. You can just think about it logically. A 5 person cyber team won't be able to run as many cybersecurity tools as a 500 person team. Does that mean that a 5 person team is worse off? Not necessarily. A smaller company also doesn't have as many services or people to protect so their risk profile is generally smaller.

The great news is that, for many small to medium-sized enterprises (SMEs), starting with Safeguards from Implementation Group 1 (IG1) is a great phase one uplift from nothing. These safeguards are designed to protect against common threats and are a solid foundation for more advanced security measures.

Now, you might be wondering about the tools needed to put these safeguards into action. Well, it's a mix of options. You can find open-source solutions, build your own, purchase from

commercial vendors, or even have them bundled into existing IT products. You should always look at the total cost of overship. IE if you add the developer costs, the licensing costs, and the hosting costs of applications you get a pretty good ballpark of what each application costs. So even though open source may have 0 licensing fees it might actually kill you on the developer costs to maintain the tool. Whereas you definitely have to look at commercial pricing to make sure you are getting your money's worth and not just paying for a brand name.

This is where a brand new document published by the Center for Information Security Comes in. They just released a white paper called the Cost of Cyber Defense: CIS Controls Implementation Group 1. This paper goes into costs and it's really interesting. Note we will have a link to it in our show notes in case you want to download it and read it yourself.

Now, let's address the cost question. CIS did some research and found that on average 5% of annual revenue went to the IT budget. Additionally of the IT budget 20% went to cyber. Thus if you opt for Commercially Supported Versions of these tools it should be less than 20% of the IT budget for any size enterprise. That's a reasonable investment for essential cybersecurity, especially considering the potential consequences of a breach.

So, if you're an enterprise looking to bolster your cyber defenses, starting with IG1 safeguards, understanding the tools you need, and realizing that it's a cost-effective move, is a smart first step in safeguarding your digital assets.

How much does it cost to implement IG1?"
To answer this burning question, let's break it down step by step. First, CIS divided the cybersecurity controls into 10 categories, including Asset Management, Data Management, Secure Configurations, and so on. This categorization helps us organize the safeguards efficiently.

Next, CIS matched these safeguards with tool types. These tools, for example, Enterprise and Software Asset Management Tools, serve multiple safeguards within a category. But here's the catch: the pricing models of these tools can vary wildly from vendor to vendor. They might charge by device, user, usage (like hours or data size), or other factors.

To make things more practical, CIS has listed three hypothetical Enterprise Profiles: Tier 1, Tier 2, and Tier 3. Tier 1 was < 10 employees, Tier 2 was 10-100 employees, and tier 3 is 100-999 employees. These profiles consider factors like sector, revenue, and employee count to provide guidance on cybersecurity spending. Even if your enterprise doesn't fit perfectly into one of these tiers, these profiles give you a ballpark figure to start with.

Now, here's where it gets interesting. CIS collected pricing information for over 200 vendor-specific tools based on the attributes of these Enterprise Profiles. While some enterprises might opt for bundled tools, open-source options, or utilities, CIS still wanted to provide an estimate for the alternative path you choose. After all, every choice comes with its own implementation and convenience costs. But remember, the costs aren't just about buying

the tools. It's also about budgeting for labor, updates, hardware or virtual assets, training, license renewals, integration, testing, consulting, advertising, and more. Cybersecurity is a comprehensive investment.

Commercial Break

If you look at the CIS Controls Cost of Cyber Defense Document on page 8 you see an interesting matrix.

The matrix shows a Tier two organization has between 10-100 total employees with an IT staff of 1 to 2 people. This type of organization usually has an Annual Revenue of $5-50 million dollars. If the IT budget is 5% of the Annual Revenue, then the organization has an IT Budget of 250K - 2.5 million. CIS found that the Annual Cybersecurity Budget averaged 20% of the IT budget. Therefore a 50K-500K cyber budget would be appropriate. Note there is some overlap between IT and Cyber Budgets. For example: Identity Management and Access Control may fall under the IT budget.

The report found the cost to implement Implementation Group 1 across 10 categories for a 10-100 person organization were the following:

1. Asset Management costs were between $690-3,896. This budget went into buying an Enterprise and Software Asset Management Tools and a Service Provider Management tool.
2. Data Management costs were between $11,192-41,918. This budget went into a Data Management Tool, a Data Disposal Tool, and Encryption tools.
3. Secure Configurations costs were between $4,710-47,494. This budget was allocated to Configuration management tools and firewalls.
4. Account and Access Control Management costs were $4,710-47,494. This budget spending went to Identity and access Management tools, Password Management Tools, and MFA tools.
5. Vulnerability Management costs were between $845-7,200. This budget spending went to Vulnerability and Patch Management Tools.
6. Log Management costs were between $632-10,866. This budget went to log management tooling.
7. Malware Defense costs were between $5,591-10,799. This budget spending went to Anti-Malware software and DNS Services/Server tools.
8. Data Recovery costs were between $2,925-11,888. This budget spending went to Data Backup and Recovery Tools.
9. Security Training were between $1,440-3,660. This budget spending went to Security Training and Awareness Tools.
10. Incident Response budget was budgeted to be 0. Essentially if the enterprises choose to do the minimum that can be achieved without tooling and would only require time to put the activities in place.

OK so if we quickly summarize this report, we see that there's a price range of $35K to $177K for the tooling necessary to perform these 10 activities. The 3 most expensive activities SMBs should budget for are Data Management, Secure Configurations, and Account and Access Control Management.

This is really interesting since it's the first security framework to publish a mapping of real world costs associated with implementing a framework. Note CIS plans to update this report as it collects more data on what tools can be used to implement groups 2 and 3 for larger organizations.

So here are my thoughts on the CIS study. First of all I really want to commend CIS for taking the time to help inform us of costs. So much of pricing information is hidden behind contracts and NDAs that it's tough to get real world data on this topic. I really hope their pricing information is accurate, because if it is good cybersecurity might be cheaper than we think it is. My fear is these numbers at face value seem a little low and I don't see the raw data behind the report to see if there were any conclusions that I don't agree with.

Second, I feel like this really makes the business case that not achieving Implementation Group 1 is going to become a real legal liability.

> For Example: I could hear an attorney making this case to a jury. The state of California has routinely warned companies that they will be held accountable for protecting and safeguarding customer data. In 2016, Kamala D. Harris (then California Attorney General) said during her speech on the data breach that CIS controls are a minimum level of security that any organization that processes personal data should meet.
>
> We have shown evidence that this company had personal data and it was expected the company would perform reasonable care of that data. Unfortunately this company chose to be negligent in terms of safeguarding PII. They did not fully meet the 153 safeguards shown in the CIS 18 controls. Additionally they did not even meet the 56 safeguards from the implementation group one which is a minimum standard of information security expected for all enterprises. Had they allocated a budget specified in the study of CIS Control Cost of Cyber Defenses they would have been within the realm of reasonable care. That being said they did not. We would like you to rule in favor of the following damages to our clients.

It makes for a compelling argument and really holds stronger accountability towards organizations.

The third thing I would point out is I don't actually think the simplification of the 18 CIS Controls down to 10 processes is helpful. I think it's actually more confusing than anything. For example: CIS control 9 is Email and Web Browser Protections. Control 9 has two subcontrols that you need to implement (9.1 & 9.2) if you want to achieve Implementation Group 1. Control 9.1 says to Ensure Use of Only Fully Supported Browsers and Email Clients. This control is

actually mapped to the Asset Management Process for Enterprise and Software Asset Management Tool. If I were to buy an asset management tool like Axonius or JupiterOne, I'm not really getting anything that patches my browsers and email clients. So I think this mapping is a bit flawed. I really wished they just would have priced the 18 implementation groups directly vs creating 10 processes that add unnecessary complexity and confusion. Item 9.2 further demonstrates this exact point.

If we look at Item 9.2 which is Use DNS Filtering Services we see that control is mapped to Malware Defense. Usually when I hear Malware Defense solutions I'm thinking in my head about tools like Antivirus or Endpoint Detection Systems. But the truth is you are probably going to get DNS filtering through a Proxy Server like BlueCoat, a Zero Trust Solution like ZScaler, or a Network Firewall. These are very different tools so I'm not sure if the costs are going to line up.

Another issue I have is fundamentally I think Implementation Group 1 still isn't correct for being a minimum standard of essential cybersecurity. For example, If you were to ask me what is the most common attack every company is going to encounter, I would definitely say phishing. Basically every business uses email so email phishing attacks are a mainstay of criminal activities. Therefore organizations should buy an email security gateway solution to secure their organization from attacks like email spoofing and malicious attachments. Note that Implementing DMARC (Control 9.5) to lower the chance of spoofed or modified emails from valid domains is in implementation group 2. Deploying and Maintaining Email Server Anti-Malware Protections (Control 9.7) is in implementation group 3. This means that if I want to stop the most common cyber attacks, implementing Group 1 isn't enough.

CIS released another white paper called, "How to Plan a Cybersecurity Roadmap in Four Steps". This Paper gives Implementation Group 1 CIS Safeguards Rate of Defense against the MITRE ATT&CK subtechniques associated with Malware a 77% score. It also says Implementation Group 3 gives you a score of 94%. Now I don't know about you, but if I'm just doing Implementation Group 1 and I'm not stopping 23% of malware, then I'm probably not sleeping well at night. I think this is why we need to take Kamala Harris's advice and adopt all 3 Implementation Groups to meet a minimum level of security.

To summarize, the CIS Controls Cost of Cyber Defense White Paper is really good. You should definitely read it. I just think if they did the pricing for each of the 18 CIS Control Groups instead of 10 processes it would be even better. It simplifies it for organizational risk decisions. CISOs could say, Implementation Group one costs 200K to stop 77% of malware attack methodologies documented by MITRE ATTACK. However if we spend 500K it gives us a 94% chance to stop known malware attack methodologies. Would you like to spend an extra 300K to stop 17% more malware attack methodologies. That makes a lot more clarity for Chief Financial Officers who control the purse strings of the organization. Note these numbers are fictional so please don't think CIS is saying 200K or 500K we are just using this as an example to explain a point.

I hope you have enjoyed today's show. Can you do us a favor and please share it. Your sharing allows us to help more people keep all of our data safe. Frankly I would love to see more conversations on the costs of implementing Cyber. Transparency is a great thing. Remember, if you want more great content subscribe to our LinkedIn page. You can get access to these documents when we first see them and be the first one to share them with your friends. Also don't forget to check out our Youtube page. We are going to do more things like show the exact tables from documents that we are referencing so it's easier to understand. Thanks again for taking the time to improve your CISO Tradecraft. We wish you only the best on your cyber journey and Stay Safe out there.