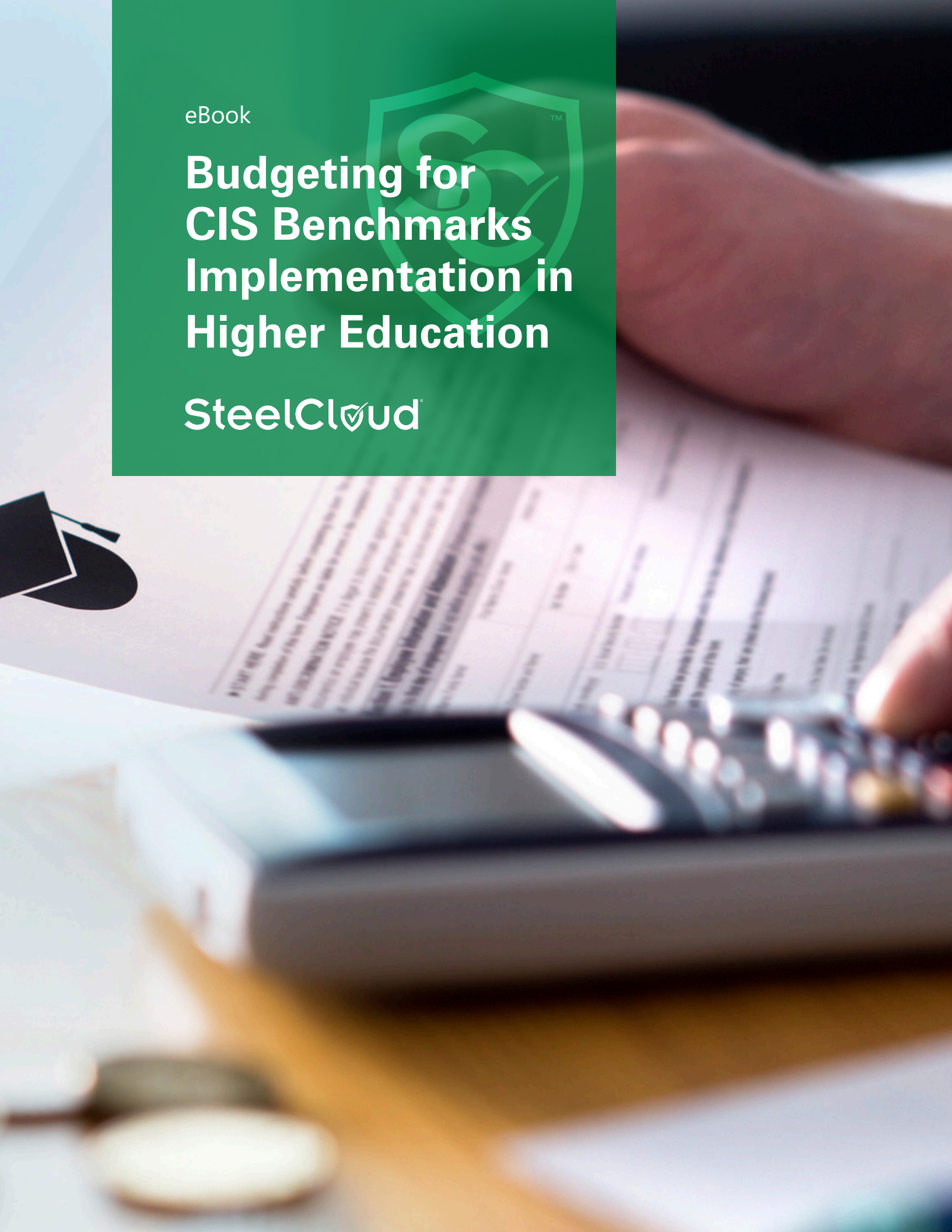


eBook

Budgeting for CIS Benchmarks Implementation in Higher Education

SteelCloud[™]





As the 2021 fall semester began, [two American community colleges](#) had to close due to cyberattacks. In June 2022, the IT system of a [university in Italy](#) was held ransom for \$4.5 million. And [Malwarebytes called out 2023](#) as the “worst ransomware year on record” for the education sector.

The average ransom for hacked data in the higher education sector is \$3.65M. And that’s just the loss of money. You can’t place a dollar amount on the loss of reputation, branding, trust, student experience and intellectual property that goes along with these attacks. Higher education is the #1 target of hackers globally with nearly 2300 attacks a week.

While colleges and universities across the nation are standing by, [waiting to see what others do about it first](#), hackers are refining their craft with AI. The industry seems to be playing a game of chicken. A game they are likely to lose. And it all comes down to money.

This eBook and the links embedded herein will give you information you can use to appeal to decision makers for the resources you need. All claims and costs are based on implementing [CIS Benchmarks](#) plus [automation](#). [CIS Benchmarks](#) offer a series of best practices that provide a roadmap to known vulnerabilities and how to fix them. [To see if CIS Benchmarks can help you, we’ve created a checklist.](#)

...the average Higher Ed
RANSOM is \$3.65M



Resource shortages keep schools from making meaningful change.

Let's face it. Cybersecurity isn't generating income for your school. So it can be hard to [justify the budget needed to implement and maintain a solution like CIS Benchmarks](#). With the average data breach costing millions, [IBM finds](#) that the average savings for organizations that use security AI and automation is \$1.76M. It could also cut weeks off the time it takes to recover from an attack.

Those are good numbers to know, because here's the grim truth: when student data is held for ransom or there is a denial-of-service attack, your school is going to pay. And it will cost significantly more than implementing CIS Benchmarks with automation. Cybersecurity is the ounce of prevention to ransomware's pound of cure.

Money isn't the only resource in short supply, though. Qualified manpower is both expensive and hard to come by. [The World Economic Forum](#) reports that, globally, there is a shortage of 4,000,000 qualified cybersecurity professionals and that number is expected to rise to 85M by 2030. If you implement and maintain CIS Benchmarks by hand, you'll need to hire the staff to do it. And that will require a much larger budget than automating CIS Benchmarks. With technology doing all the scanning and remediation for you, you can easily implement CIS Benchmarks with the staff you have on hand.

Crunching the numbers to see how much CIS Benchmark automation costs.

As mentioned previously, the average cost of a data breach in higher education is \$3.65M. Maybe you have to pay a ransom to get your data back. Maybe you lose research or other data, impacting grants and competitive standing. Maybe you lose business, enrollment or donations as a result. There is likely going to be a significant loss of service and system availability, as well as a loss of trust. And all of that is before the actual costs of restoring your system.

[Here's a rough estimate of how much it would cost to implement CIS Benchmarks](#). Spoiler alert: It's less than \$3.65M. How much it costs YOUR institution depends on a number of factors, such as:

- ✓ The size and complexity of your system
- ✓ Whether you'll implement manually or through automation
- ✓ And how you'll maintain your security posture after implementation



Now that you know the costs of CIS Benchmarks implementation, the next line item is labor. You could hire a team of dedicated specialists to implement and maintain compliance with CIS Benchmarks manually. Or you can automate and reduce your year-over-year costs significantly. As far as the costs of automation, [reach out SteelCloud for a quote](#). Our technology is [the only technology](#) proven enough to be recommended in the [CIS CyberMarket](#).

Pleading your case to leadership.

With a rough idea of what you're looking at, it's time to make an appeal to leadership. Here are four arguments that should get their attention:

- ✓ **Your school doesn't want to be the topic of negative headlines.** Leaders don't want to explain why innovation took a hit when research was stolen. Or why student success is made more difficult by system unavailability. If your school takes a major hit, they will have to answer questions. And while they may come up with a spin on it, everyone will assume it's because their cybersecurity program is underfunded and insufficient.
- ✓ **Breaches impact your pillars.** Innovation and student success are common "pillars" or goals universities emulate and sell to prospective students and donors. Look at the pillars your leadership holds dear and demonstrate how they are at risk without the funds to tighten cybersecurity.
- ✓ **Cautionary tales get people thinking.** Have a couple of real-world stories on hand like the [University of Pisa \\$4.5M ransomware attack](#) or the [University of Minnesota database hack](#) that went undetected for two years. Give them the broad brush of things that are happening at colleges and universities so they can see the breadth of risks and the frequency at which they are happening.
- ✓ **Leaders love statistics and averages.** Arm yourself with the statistics in this eBook and other statistics you can find. Higher education is the #1 target for hackers worldwide, partly because you aren't given the proper budgets.
- ✓ **Your budget should be tied to revenue.** CIS recommends an IT budget that is 5% of overall revenue, with cybersecurity getting 20% of that money. If that is less than you are getting, make your case using that formula. CIS is the industry leader when it comes to best practices, culling their insights from the global cybersecurity community.



Automation and the role human error plays in cybersecurity.

As mentioned before, automation is more affordable and faster than implementing CIS Benchmarks manually, plus there is zero human error. [According to IBM](#), human error plays a role in 95% of security breaches. Now, some of that is user error and phishing, but some of it is also mistakes made by overworked, highly stressed cybersecurity professionals. [Gartner predicts that, by 2025](#), more than half of cybersecurity incidents will be directly tied to a lack of talent or human failure in cybersecurity.

[Among other benefits](#), automation can reduce your time and effort burden by 90%. And you'll likely be finished with your work—using your current team—by the end of the semester. Which means that every time you update your system in any way (even simply adding new users) just a push of a button ensures you stay in compliance. You'll also get new technologies and applications online faster than you would using manual means. Which could make a difference at every touch point in your system, from research to coursework. Automation will scan and remediate every endpoint in your system in about an hour. Along the way, you'll be reducing your costs by at least 70%.

Take the guesswork, high costs and headache out of cybersecurity.

CIS Benchmarks take the guesswork out of securing your system to recommended standards. [And automation takes the headache out](#). Instead of the months it takes for a team of humans to implement CIS Benchmarks by hand, automation can do it in an hour. It can secure your system and keep your baselines hardened in perpetuity with the team you already have. [It can also save their sanity](#).

SteelCloud's ConfigOS is a patented automation tool used to [implement CIS Benchmarks in the education sector](#), as well as anywhere else security counts. It scans your system for CIS Benchmark-identified vulnerabilities, then fixes the vulnerabilities and cleans up any mess it left in its tracks. It literally pays for itself from its first use and not only makes CIS-level security possible in tight budgets, but also eliminates the human error of the long, laborious process of securing your system by hand.

Once you start looking into it, you discover CIS Benchmark implementation is a really big job. But the tools and expertise are available to get you through the process unscathed. If you'd like to talk to SteelCloud about including a CIS Benchmarks automation solution (and ruining the day of some hacker who thought you'd be an easy payout), schedule a meeting and demo with us today.



About SteelCloud

SteelCloud has been automating STIGs and CIS Benchmarks for well over a decade and our [ConfigOS cybersecurity automation software](#) has been repeatedly proven in highly sensitive government agencies, complex corporate environments and [Higher Ed](#). We are also [a trusted CIS certified vendor](#).

We understand if you're skeptical considering the source, but our experience in the industry has shown that even the most sophisticated and skilled cybersecurity teams in the nation can't go it alone. Some try. But most turn to SteelCloud and ConfigOS to simplify the chaos. [We are the right solution at the right time for CIS Benchmarks implementation in Higher Ed.](#)

Take a step forward in your journey by downloading our [CIS Benchmarks Compliance Success Guide](#) for a holistic look at the challenge. Then [schedule a free, no-obligation demo of ConfigOS](#). See how it works. Chat a little about CIS Benchmarks. Get some ballpark costs. And learn how you can make the resources shortages and mental overwhelm of this massive undertaking a thing of the past.

For more information call (703) 674-5500,
email info@steelcloud.com or visit www.steelcloud.com.