

**Cybersecurity Isn't Just IT Anymore: Why It Should Be at the Center of Business**

Hussein Al Saffar

Department of Cybersecurity, Old Dominion University

CYSE200T: Cybersecurity, Technology, And Society

Professor Matthew Umphlet

April 12, 2025

**(1) Here's an issue about the development of cyber-policy/infrastructure and my position on it.**

If there's one thing that's become clear in the last few years, it's that cybersecurity can't just be something that lives in the IT department anymore. As companies get more digital and more connected, cybersecurity has become a core part of running a business—right up there with finance, operations, and marketing. I believe it should be treated as core infrastructure, not as an afterthought or something you only deal with when there's a problem. In other words, cybersecurity needs to be part of how we design and manage every piece of a business—not just the tech stuff.

**(2) Here's some concrete evidence and how it supports my position.**

Right now, a lot of businesses still treat cybersecurity like a fire extinguisher: something that's useful to have when something goes wrong, but not something they think about every day. But that mindset is seriously outdated. Just look at how many big-name companies Target, Equifax, even healthcare systems—have had data breaches that didn't start with some hacker in a hoodie breaking into code, but with a simple mistake like an employee clicking the wrong link. These aren't just tech problems; they're people problems, leadership problems, policy problems.

The World Economic Forum's 2023 cybersecurity report even says that cyber risk is now a "business risk," not just a tech one. And it makes sense. When a company gets hacked, it affects more than just its servers. It can lead to lawsuits, drops in stock prices, and a total loss of customer trust. So the idea that cybersecurity can stay tucked away in IT doesn't really work

anymore. It has to be part of HR training, legal compliance, financial planning, and even branding and PR.

**(3) Rational, persuasive writing—arguing using legitimate argumentation.**

Now, I get the argument that not every business has the resources to fully integrate cybersecurity into every department. Especially for smaller companies, that kind of overhaul can feel overwhelming and expensive. But the alternative—doing nothing or doing the bare minimum is way more expensive in the long run. Cyberattacks can literally shut down businesses. And the good news is, integrating cybersecurity doesn't have to be high-tech or super complex. It can start with things like strong password policies, regular training, or having leadership involved in data protection conversations.

Plus, building a company that values cybersecurity sends a message to employees and customers that you're serious about protecting them. And in today's world, where personal data is everything, that kind of trust is priceless.

**(4) Labeling one paragraph where I clearly accomplish this item.**

There's also an ethical side to all this. Businesses collect tons of data about their employees, their customers, their partners and they have a responsibility to keep that data safe. When a company doesn't take cybersecurity seriously, they're not just risking their own business; they're putting other people at risk too. And that's a problem. Trust is hard to build and easy to lose. So even if it's not required by law (yet), I think it's just the right thing to do.

**Looking Ahead: What Happens If We Don't Make This Shift?**

Here's where I worry about the long-term. If we keep treating cybersecurity like a side project instead of a foundational part of doing business, we're going to see bigger and more dangerous failures. As technology continues to evolve, think AI, smart devices, digital currencies the risks grow too. One weak link in the system could cause damage far beyond one company.

We've already seen how a ransomware attack on one company can ripple out into things like hospital delays or supply chain problems. These aren't just hypotheticals anymore. And as much as we want to believe we can fix problems as they come, that approach just doesn't work with cybersecurity. We have to build systems that are secure by design, not just secure after the fact.

**Wrapping Up: A Realistic but Urgent Take**

So here's where I land. I believe cybersecurity needs to be treated as a core part of how businesses are structured and run. The evidence is everywhere from the rise in data breaches to changing consumer expectations. And while it might take time and money to make that shift, not doing it is a lot riskier.

That said, I know this isn't simple. Not every business has the same resources. Some industries are more regulated than others. And let's be honest some leaders still don't fully understand what cybersecurity really means. There's no one-size-fits-all fix. I don't have all the answers, and I don't think anyone does. But I do know that ignoring the problem or pushing it

off to “the tech people” won’t work anymore. We’re in a moment where businesses can either evolve or get left behind. Making cybersecurity a part of the foundation, not just a patch or a plug-in is the best step forward.

## References

*Cyber Security Awareness Training Platform*. CybeReady. (2025, March 13).  
[https://cybeready.com/?cat\\_ID=244](https://cybeready.com/?cat_ID=244)

AdminAI. (2024, December 8). *Navigating plea bargains: Weighing the benefits and risks in criminal cases*. Attorneys.Media | Watch Attorneys Answer Your Legal Questions | Local Attorneys | Attorney Interviews | <https://attorneys.media/plea-bargains-criminal-cases/>

Horrigan, B. L., Editor, E. M., Marks, M., Director, P., Shacklett, M. E., Data, T., Writer, T., Networks, W. G., Grady, J., Analyst, P., Gillis, A. S., Editor, T. W. and, Awati, R., Burns, S., Waldman, A., Writer, N., Bigelow, S. J., Editor, S. T., Wright, R., ... Rosencrance, L. (2025, April 30). *Cloud security*. Cloud security | Resources and Information from TechTarget.  
<https://www.techtarget.com/searchsecurity/resources/Cloud-security>