The impact of our cybersecurity systems is profound, however, it’s important to remember how little control most individuals actually exert of their cyber presence. This is part of why I think there is a need for a stronger, more responsible, authoritative body to help citizens in cyberspace as it’s relatively clear our current legislators and authorities have fallen short or failed us too many times.

Not only are citizens affected by this ineptitude, though, even the businesses they are a part of are affected. Many already probably hear about this, though, as security and data breaches seem to be constantly in the news. A security breach can damage or even kill a company wholesale. Security breaches have both immediate material consequences, and more latent and long term effects. The long term effects are a little less convincing, but nonetheless still very real. One that is often talked about is lack of trust. I almost never put more stock into this trust idea than I have to, but in this instance, especially in critical industries, it is very serious. In these cases not only do you lose out on customers and partners, but governments and regulators may step in, shareholders may leave or become unruly and demand change, and overall the stability of the company can come into question. The efficacy of legislators when they step in is in question, though, as the only reactions I’ve ever had to a legislator lead cyber initiative that actually was enacted was either “That might be the opposite of what we need” or “Well, it’s about time”. In terms of immediate concerns, there are things like injuries and even loss of life due to sabotage or failure. There are also immediate losses if the data affected is lost or damaged in the breach. The time spent both recovering and being affected by the incident is another immediate problem that arises. Overall, the impacts are major. Companies regularly see around 350,000 damage per breach, with a breach per year being very common. Larger companies, per the article, could see at 500,000 in damages or more. When it comes to preparedness, in all likelihood, most companies are not prepared. Non-critical companies are not required to do a number of things, with 60% of companies not being compliant with government regulation, and no widely recognized entity in charge of regulation and standardization is there to pick up the slack. A very important figure is that 81% of companies surveyed are not required to disclose these breaches, so I believe most of the time, they are gambling on their potential breaches not being reported enough to cause major damage. Despite this most companies seem to believe they are prepared for an attack despite the fact that of the companies surveyed, only 2/3rds are implementing anti-malware solutions at endpoints, only about half use intrusion detection and prevention systems, only 44% use access control, and so on. These facts taken together paint a picture of a scattered, decentralized set of companies doing a passable, but very risky job of protecting their systems. With huge losses common and attacks even more so, these companies non-compliant with regulation, without basic defenses like anti-malware and access control, and without help from a central body, should likely be implementing more measures to both protect and defend their systems I believe. If a central authoritative body were to step in, they could at the very least provide massive assistance with these problems.

Let’s shift back to citizens, though, as it can help us see the full scope of the problem here. See, not only are the physical systems in question (like the ones that allow for data breaches), but the policies in place are also being thrown into question. One key policy that is as disjointed and scattered as they come is password policy. Everyone knows the pain of having 30 different passwords for 20 different sites. This pain is compounded in that every site seems to have its own policy and own idea of what secure means. Surely one must be more correct than the other, though. If you aren’t in the field though, then you would have no idea what more correct means though, as some companies don’t even require traditional passwords anymore, while some require 15 characters and all manner of symbols. Well let’s look at one key trend in identity management to see just what “more correct” might actually mean, the shift away from the old model of user responsibility for complex passwords, into a more provider based system using two-factor or biometric authentication. Currently, when we look at the age demographics, it paints an interesting picture. We're somewhat stuck at a crossroads here, where younger generations are more often enrolling in more secure policies, but are not following best practice in the areas that still use traditional passwords. About half of all individuals ranging 45 and over in the survey group seemed to use complex passwords. With 18-24 year olds, it was less than 40%. In the same vein, 28% of 45-55 year olds and 31% of 55+ individuals reused passwords, while 42% of 18-24 year olds reused their passwords (which as we already have seen may not be complex enough). These practices likely compound, making one breach of a simple password even more deadly. This paints a sorry picture for younger, supposedly more tech-savvy individuals, however it doesn't quite paint the whole picture. The same study found that younger individuals are much more likely to use advanced security techniques like biometrics and two-factor authentication. This seems to ask, would we rather users focus on making strong, one per account passwords, or we would, we rather put our resources into pushing for two-factor authentication and biometrics to give us a more complex and advanced security structure. When we look at global trends in biometrics, things also make for a much more complex web we'll have to untangle. In general, it seems as if US citizens are the most aware of data breaches and their impacts, but also seem to be the least willing to try and implement biometrics into any aspect of their life, barring potentially Apple ID to unlock their phone. Interestingly enough, though, as of right now the US seems to be doing slightly better in multifactor authentication willingness, even if it's lagging far behind in other advancement metrics. APAC countries seem to be the most willing to use, interested, and comfortable using biometrics, seem to be the most understanding of its potential flaws, and are the most willing to use it in different aspects of life. The EU countries tend to be somewhere in the middle, using multifactor authentication and biometrics less now than even potentially US citizens, but also has a higher interest and understanding regarding them than US citizens, but less than APAC citizens. FIDO seems to be a leading organization rallying to the charge against password use. Their ideals are that passwords are less secure, not any more scalable, and potentially even less convenient and more intrusive than two-factor and biometric solutions. Their eventual goal seems to be liberation from passwords, and they hope to establish a web of industry partners to set the standards for a unified two-factor authentication implementation standard across the net. One could only imagine how much more efficient it would be to already have a central authority in place to standardize these practices, instead of groups like FIDO trying its hardest to somehow bring together a loose conglomeration of like-minded groups.

So we know the need is there for both policy control, systems control, standardization, and authoritative consequences and regulations for certain practices. To really round out just how dire this need is, though, we can look the landmark cyberstalking and harassment study conducted in 2013 by Steven D. Hazelwood & Sarah Koon-Magnin. My takeaway from the study is that it clearly seems that our legislation, justice systems, and support structures are not designed in such a way that they can respond to these quick cultural and technological changes in an adequate amount of time to sufficiently protect us as a whole. For instance, at the time of this study's publishing, Nebraska did not have legislation concerning cyberstalking and cyber harassment. Likewise, states such as Arizona did not have competent or sufficient legislation that could be comprehensive enough to be effective. It seems to me at least that the devolved powers of states should not be so that in one state you can be harassed with no meaningful way to respond effectively and protect yourself in a legal manner. When the states were set up as a concept, there were many who argued in its favor for a number of reasons. Personally, however, I see no good reason why in the very same country one person could legally have at least competent protections from cyberstalking, and across a subnational boundary another person might not. This argument can be extended to all manner of things. Some states have a more humane drug law system set up, while some states have literally thousands upon thousands of non-violent offenders holed up in a jail cell (with years of their life being stolen from them) for a non-violent marijuana possession charge. Years ago, the same could be said about marriage rights. In one state you may be able to marry your partner, but a few miles away across a state boundary it would be impossible. This all speaks to me that our archaic systems we have set up are not nearly sufficient in doing the jobs that we expect them to do. Put clearly, in 2013 Nebraska really should not be allowed to not have cyberstalking and cyber harassment legislation on the books. The lawmakers, in my opinion, should be put on trial and investigated, as real lives are at stake here over serious matters like this. To borrow a concept discussed in the study, no reasonable person would agree that cyber-stalkers and harassers should be allowed to freely commit crimes due to incompetence, corruption, ineptitude, malice, or a combination of them all present within those responsible for seeing that action is taken against them.

The conclusion here is that cyberspace, in all matters, from policies, practices, legislation, systems, consequences, etc., seems to be a new wild west for society. No central authority is there to provide consequences for bad actors, or for even just criminally negligent ones. Policies are scattered and inconsistent, harming security as a whole. Businesses, citizens, states, and entire nations are affected. We live in a global world, with all sorts of global rules that are only becoming more widespread due to this technology itself. Despite that, we are as fragmented as ever when it comes to implementation and security in cyberspace. While clearly the new advances in cyberspace have had a positive impact on our society, as long as it remains completely unregulated, uncontrolled, and unrestrained the consequences will continue to mount. Our legislators have failed, our businesses often cross us, and many of the groups trying to fix the problem are not equipped to do so. So I believe it’s time to act. We have to stand up and force action, either by pressuring those in power, removing those unwilling to solve the problem, or, likely the only real option that has the power to provide the results we need, destroying the old systems in place and bringing in new ones to match our new reality. Many may see this as a problem using our current systems, we just need more time, or more efficient leadership. To them, I would simply point out we’ve been dealing with this decentralized and dis-unified cyber-world since the inception of cyberspace itself. This current problem is fruit that bore on the tree of inept and decentralized forces. We already live in that reality, and as many would agree with, we do not quite like the results. The password policies, the data breaches, the inept cyber violence laws, the sets of rules that apply to one entity and not another, it’s all things I think we all would wish to change. We have been in that reality for some time, so in changing it for the better, we have nothing to lose but our chains (and maybe some 30+ passwords we can’t remember).

References

Hazelwood, Steven D. and Sarah Koon-Magnin. “Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis.” *International Journal of Cyber Criminology* 7 (2013): 155.