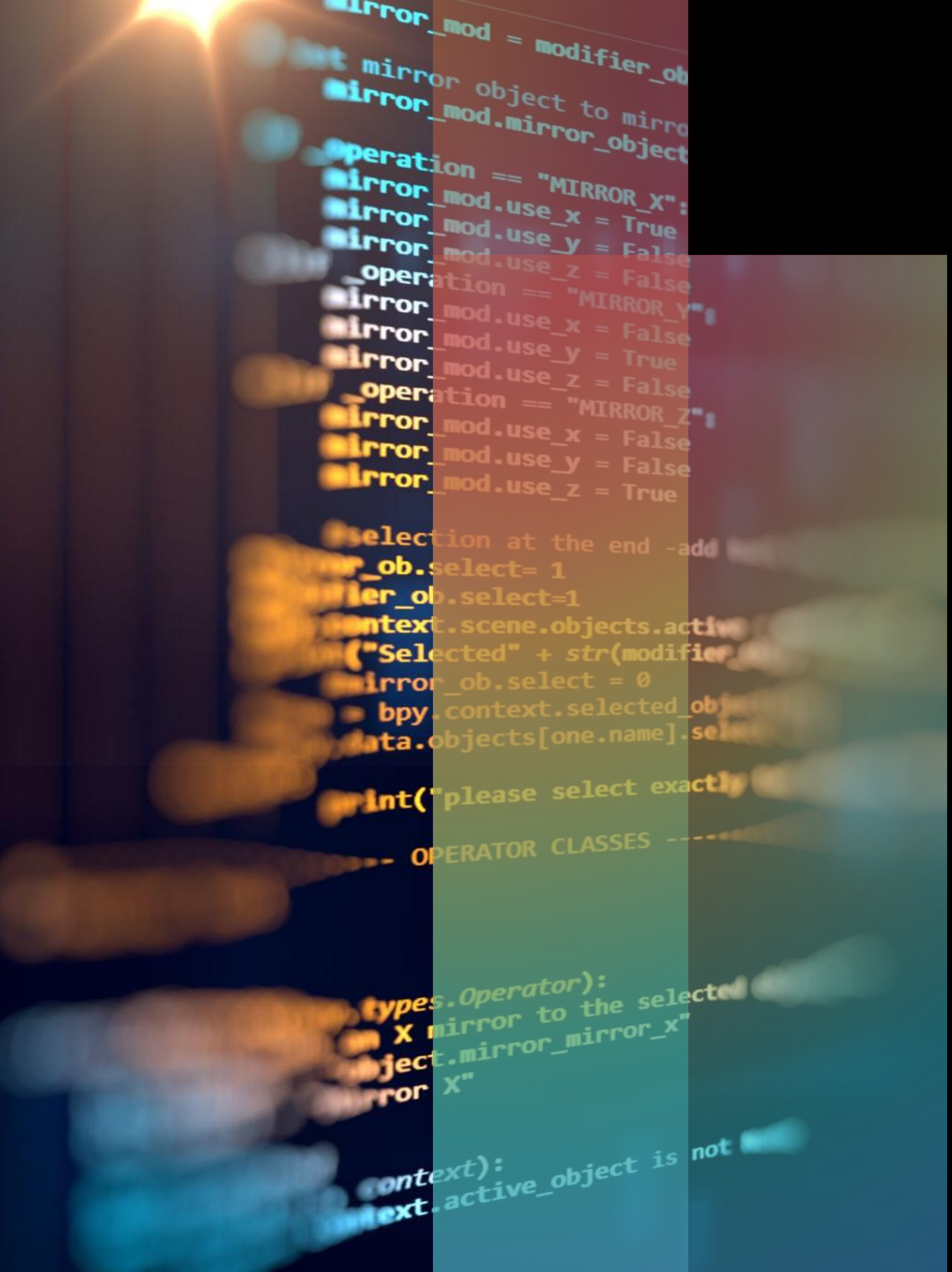


Cybersecurity A2 Group #1

Cybersecurity is such a huge global industry now as we move into an era where are lives are reliant upon technology applications and IoT networked systems. Cybersecurity enables us to protect our critical systems and sensitive information while we navigate through life and business. As threats can come from both inside and outside of personal and company structures, we need cybersecurity to help us combat these threats and maintain a level of control over our online presence and information.

https://www.myfrugalbusiness.com/2020/12/different-types-of-cyber-security.html

The link is to the blog linked above is by Bootstrap Business they write about three different areas of cyber security.

- *Cloud security*: storing information online and sharing it. It can make us vulnerable and put us at risk.

- *Network security*: this includes using VPN's, firewall protection and multi-factor authentication on our devises that we use each day.

- *Application security*: we all have apps on our phones. Keeping our information on those apps safe, stored and maintained well is important.

The state of the cybersecurity industry is always changing and evolving, and some might say not fast enough. Cyber breach issues used to be relatively low and uncommon but now you can talk to just about anyone and they will have a story to share about breaches at work, home or in their social networks. One of the biggest evolutions to cybersecurity is threats to nations.

https://ifflab.org/the-5-latest-cyber-security-technologies-for-your-business/

This cybersecurity blog by the Incognito Forensics Foundation says, "*the United States has recently declared cyber-attacks to be a greater attack to the country than terrorism*."

This is very alarming, and we should all be concerned. The article goes on to talk about how targets have changed from being small and petty to more malicious intent with sever consequence for nations and countries all over the globe.

Other industries that have been majorly impacted by cyber-attacks are manufacturing, healthcare, oil and gas, intelligence, military, banking and other financial systems, politics and let us not forget education.

In-fact I was at an online symposium for cybersecurity in the oil and gas industry and it was hacked.

These industries have huge spending allocations to keep their systems and information protected. From hundreds of millions even low billions are the figures we are talking about each year that these companies must invest to protect themselves and their consumers/customers.

My experience with multinational companies has taught me that it is not just the money involved it's the people they hire to maintain cybersecurity that has changed.

Before companies would not have to go to greater lengths as they do now to protect information. Now it requires teams of people mostly software engineers, full time to maintain security.

Cybersecurity has become a skill that is required for most tech jobs now as most jobs have an online component that requires basic security knowledge to protect information as they create, develop, store or move information online.

Just the cost and staffing expenses of maintaining security alone have pushed many companies out of the market. They do not meet regulations; cannot afford that kind of investment and they cannot protect their consumers.

This is having a huge impact on who is in the marketplace and what companies will dominate in the future. Those companies that transitioned early have kept their position and protect their information well, making information they collect even more valuable.

As for small businesses I really do feel for them as they do not have the budget to mitigate online threats like bigger companies.

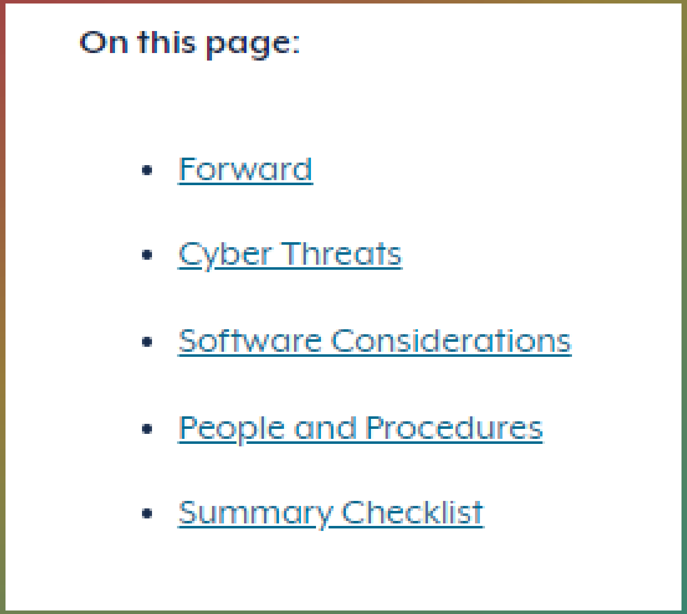
https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide

This link is a guide for small businesses provided by the Australian government.

It gives a general overview of common attacks and educates small business owners and individuals on what they can do to be pro-active in this cyber age. It talks about:

- *ransomware*
- *phishing*
- *malware*
- *multi-factor authentication*
- *access controls*
- *passphrases*

These things are essential for people who are online. I think that children should be taught about the importance of cybersecurity and protecting your information from a young age at school.



On this page:

- Forward
- Cyber Threats
- Software Considerations
- People and Procedures
- Summary Checklist

The impacts of the cybersecurity industry and its evolution on the world have been both refreshing and scary.

More information is readily available to the public now therefore exposing bad characters and their systems faster. This also means that bad characters are evolving fast also, and this is a big problem for the cybersecurity industry.

Can they really guarantee anyone is safe online?

https://www.youtube.com/channel/UChO_bPg4QOWxSOzH4OYw3Tg

YouTube pages like “Australian Cyber Security Center” provided in the link above are a great way for people to get information and stay connected to what is currently happening.

To the left is a screenshot of what options you can choose from to explore their website.

https://www.techradar.com/au/news/what-is-the-future-of-cybersecurity

Jacob Parker from the techradar.pro blog writes about these key ***future*** areas of cybersecurity. Next to it I share my opinion.

- *AI will be at the core of all cybersecurity systems:* *"Future cybersecurity software and personnel will be forced to develop techniques to detect and counteract AI corruption attacks."* I already see this playing out right now. The people who run AI and the big tech companies have a huge monopoly, realistically they have dominance in not just the marketplace but humanity. Australia really needs to invest in AI a lot more. I feel like we are 10 years behind.

- *cybersecurity will focus of warfare threats:* State run threats is something I think we should all be worried about not just on a country-to-country basis but a country to individual level of attack also. I predict that will be happening more as foreign intelligence targets key people. Other countries have huge amounts of people dedicated to cyberwarfare such as North Korea, Vietnam, Russia, India, Iran etc. Australia has not dedicated the same resources into mitigating this situation nor do they have the manpower to compete I think it is going to be a problem.

- *more hacking:* Is inevitable and out of control. I do not know a single person who has not been hacked. Do we accept it as a new standard? How can we possibly stop it? These are questions I certainly ask regularly. Jacob raised good points about poorer countries and communities and their reasons for hacking being no jobs, less income etc. Poverty is growing and the wealth gap is widening as this has been such an incredibly huge wealth transfer. As the cost of living rises and wages remain the same this hacking issue will only become more saturated making our online experiences unsafe for everyone.

- *cybersecurity talent become essential :* The shortage of skilled workers in this area is growing daily. In Vietnam there were massive shortages of workers, and the work did not get done. The workload for those in the industry is too much to bear. The exponential growth of the cybersecurity industry could perhaps be elevated by tech itself doing security…but is that safe having computers running security for humanity?

- *legacy tech will continue to be an issue :* I agree with Jacob because I have seen first had the choices that companies make to save money by cutting on security and that will continue to be an issue.

Thank you.

Cybersecurity A2 Group #1