Op Ed: When it comes to cybersecurity, lawyers don't need to embrace Dr Strangelove

Drew Gough*

ABSTRACT

This Op Ed, a conversation starter for the Canberra Law School 2020 symposium on artificial intelligence and law, critiques recent expressions among the information technology community that 'cybersecurity is not very important'. The Op Ed suggests that systemic improvement in information practice is both necessary and achievable in the emerging IoT economy; cybersecurity involves forewar-looking law reform rather than being left to accountants.

I INTRODUCTION

In *Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb* (1964) Stanley Kubrick offered a mordant satire of inept US politicians, gung-ho generals and policy advisers ready with assurances that in 'thinking about the unthinkable' life after Armageddon might not be too bad.[1] We should relax, trust the experts and learn not to worry about cataclysm or simply have fun playing 'duck and cover' under beds, school desks and other defenses. In the age of Trump and Little Rocket Man that denialism – denial about the likely incidence and severity of harms and, as importantly, about the responsibility of people in positions of authority – is timeless.[2]

It is relevant to private and public thinking about digital harms and responsibilities. The past two decades have seen declarations that cyberspace ends the viability of the nation state, a superseded artifact from the era of coal, crinolines and big oil ... something destined to evaporate like a mothball.[3] We have seen assurances that 'your privacy is gone, so get over it'[4] and that if you have nothing to hide you have nothing to fear, a trope that assumes both a utopian openness to surveillance by the likes of Cambridge Analytica and the capacity of the government to ensure that nothing *need* be hidden.[5]

*Drew Gough workis in the information technology sector and guest lectures at the University of Canberra

[1] Peter Krämer, *Dr. Strangelove or: How I learned to stop worrying and love the bomb* (British Film Institute/Bloomsbury, 2017).

[2] Michael Specter, *Denialism: How irrational thinking harms the Planet and threatens our lives* (Penguin, 2009); and Herbert Lin, 'The existential threat from cyber-enabled information warfare' (2019) 75(4) *Bulletin of the Atomic Scientists* 187.

[3] Nicholas Negroponte. *Being Digital* (Vintage, 1995), 238. Seealso John Perry Barlow, 'A Declaration of the Independence of Cyberspace' in Peter Ludlow (ed), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (MIT Press, 2001) 27.

[4] Polly Sprenger, 'Sun on Privacy: 'Get Over It'' (2009) 7(1) *Wired* 34.

[5] Matt Campos, 'Cambridge Analytica, Microtargeting, and Power: "A Full-Service Propaganda Machine" in the Information Age' (2019) 13 *Trail Six* 24. See more broadly Vito Laterza, 'Cambridge Analytica, independent research and the national interest' (2018) 34(3) *Anthropology Today* 1; Brittany Kaiser, *Targeted: My Inside Story of Cambridge Analytica*

In this Op Ed, I want to question a strain of thinking in law and practice about cybersecurity, in essence claims that everything we have been doing has worked so far, so why need to make a 'quantum leap' in cybersecurity an all-consuming goal. Thought is provoked by 'Cybersecurity Is Not Very Important'[6] from mathematician Andrew Odlyzko, one of the more incisive analysts of the financial and technology bubbles in the first years of adoption of railways.[7]

Odlyzo contends that there is no need to radically change our approach to IT Security, and that we if accept that all systems can be breached and plan for that event, we will be at peace with ourselves. In an introduction that might delight Kubrick and Dr Strangelove, he comments

> It is time to acknowledge the wisdom of the "bean counters." For ages, multitudes of observers, including this author, have been complaining about those disdained accountants and business managers. They have been blamed for placing excessive emphasis on short-term budget constraints, treating cybersecurity as unimportant, and downplaying the risks of disaster. With the benefit of what are now several decades of experience, we have to admit those bean counters have been right. The problems have simply not been all that serious. Further, if we step back and take a sober look, it becomes clear those problems are still not all that serious.[8]

This however assumes that the people on the other side of the cybersecurity equation share a similar philosophy. That assumption is viatiated through experiences such as the long-term and large-scale security failure at the Australian National University and problems with health, entertainment or other platforms such as Sony. Why should not we try to shift the Overton window when it comes to cybersecurity, thereby fostering greater agency on the part of consumers and greater awareness (with consequent liability) on the part of regulators and solution/hardware vendors or other stakeholders?[9] Could we have a more nuanced conversation on the part of legislators and legal practitioners, including readers of the *Canberra Law Review*?

and How Trump and Facebook Broke Democracy (HarperCollins, 2019); and Christopher Wylie, *MindF*ck: Inside CambridgeAnalytica's Plot to Break The World* (Profile, 2019).

[6] Andrew Odlyzko, 'Cybersecurity Is Not Very Important' (2019) Ubiquity (June 2019) 2. See also Peter J. Denning, 'The Profession of IT: An interview with Andrew Odlyzko on cyber security' (2019) 62(9) *Communications of the ACM* 28.

[7] See for example Andrew Odlyzko, 'Novel market inefficiencies from early Victorian times' (2017) 24(2) *Financial History Review* 143; and This time is different: An example of a giant, wildly speculative, and successful investment mania' (2010) 10(1) *B.E. Journal of Economic Analysis & Policy* 60.

[8] Odlyzko (fn5), 1. See also the less polemical Andrew Odlyzko, 'Life, Law, and New Privacy in a World of Illusions and Manipulations' (2019), https://ssrn.com/abstract=3434221

[9] The range of ideas or concepts considered acceptable in political or public debate, named after Joseph P. Overton. See Nathan J Russell, 'An introduction to the Overton window ofpolitical possibilities', https://www.mackinac.org/ 7504; and Jeanna Matthews and Matt Goerzen, 'Black Hat Trolling, White Hat Trolling, and Hacking the Attention Landscape' in *Companion Proceedings of The 2019 World Wide Web Conference* (ACM, 2019) 528.

One response to Odlyzko is that we should both question rhetoric about 'cybergeddon'[10] and try harder, try more often and try more creatively to identify and address opportunities for systemic improvements in information practice. In the United States many believe congresswoman Alexandria Ocasio-Cortez's "Green New Deal" – as much a matter of changing public discourse as it is of specific initiatives – is not achievable, thus tagged by many detractors as too ambitious or unnecessary. Others believe that aiming for such a lofty goal is the only way to achieve real change: even if they don't reach their targets, they will still have made incremental improvements that when aggregated represent meaningful change and result in public benefit.

The same thinking should be true for cybersecurity and lawyers have a role to play in building understanding.

If there are harms, in that view, the benefits of forward-looking best practice may offset any inconvenience and the cost of averting harms will be incommensurate, a manifestation of a social licence underpinning all digital platforms (which exist in a legal framework rather than as abstractions). That view is at odds with a neoliberal risk allocation schema in which administrative convenience is privileged and in which it axiomatic that law should fundamentally reduce, if not eliminate, burdens on government agencies and corporations such as Facebook, in other words entities that should be left alone to get on with public administration and making money (irrespective of whether that benefits Piketty's 1% or society at large).[11] Recommendations by the Australian Competition & Consumer Commission in its 2019 *Digital Platforms* report suggest that some Australian government agencies have a sense that corporate behavior does need to be shaped through statute law – rather than being left to Odlyzko's exasperating beancounters and consumers – and that there is indeed scope to provide that regulation in ways that address the regulatory incapacity of some agencies (notably the Office of the Australian Information Commissioner) without unduly crimping investment for innovation.

Odlyzko offers a bracingly contrarian assault on doctrines about cybersecurity – a case of 'not much to see here, folks, so move on' – and about the agency of different stakeholders, from ordinary consumers through to specialist government agencies charged with maintaining the stability of the internet and averting the cataclysmic collapse depicted in Robert Harris's new *The Second Sleep*.[12]

[10] Jason Healey, 'The Five Futures of Cyber Conflict and Cooperation' (2010) Georgetown Journal of International Affairs 110; Misha Glenny and Camino Kavanagh, '800 titles but no policy—Thoughts on cyber warfare' (2012) 34(6) *American foreign policy interests* 287; and Sean Lawson and Michael K. Middleton, 'Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016' (2019) 24(3) *First Monday*.

[11] Thomas Piketty, 'About capital in the twenty-first century' (2015) 105(5) *American Economic Review* 48; and Mark Zandi, 'What Does Rising Inequality Mean for the Macroeconomy' in Heather Boushey, J Bradford DeLong and Marshall Steinbaum (eds) *After Piketty: The Agenda for Economics and Inequality* (Harvard University Press, 2017) 384.

[12] Robert Harris, *The Second Sleep* (Hachette, 2019).

In preparation for the Canberra Law School's 2020 symposium on artificial intelligence and the law I want to dissent from Odlyzko's analyses, while acknowledging that the occasional dash of cold water has a salutary effect in deepening public consideration of information technology frameworks rather than merely generating headlines.

A Zombie Army of Smart Toasters?

Picture if you will, hordes of shambling zombified IoT-enabled kitchen appliances roaming the cyber wastelands … devouring DNS services, content delivery networks or ISP's with indiscriminate abandon. All at the whim of some shadowy dark force that controls millions of these poor unassuming devices that, if they were sentient (unlike the devices I discussed last year) and wanted anything, wanted only to let you know via a smartphone app that your toast was 30 seconds away from being ready, or that you were indeed out of juice.[13]

IoT, short for 'Internet of Things', refers to any device connected to the internet via an inexpensive Wi-Fi or cellular network interface card with some form of onboard processor and operating system. This has led to an explosion of internet connected devices, from fridges to deadbolts and hospital pathology equipment and university printers. It seems if you can 'connect', with apologies to the exhortation by E M Forster, they are. Gartner predicts that by 2020 there will be over 26 billion IoT connected devices. IoT security has not been high on the list of many manufacturers who simply wish to get a 'smart' version of their appliance (whether it be television, toaster, lightbulb, or juicer) to market. The upshot of this that there are suddenly now hundreds of millions of devices which are connected to the internet and running minimal security, if any at all.

Odlyzko contends that security practices are sufficient[14] and this is evidence that the long feared 'Cyber Pearl Harbor' or 'Cyber-hurricane Katrina' is unlikely to happen. Without any disrespect for Odlyzko's beancounters – some of whose fathers might have been responsible for regulation of the Ford Pinto[15] and other under-investment in product safety – I disagree with Odlyzko's contention. Cyber disasters have indeed happened and are happening. Lawyers, accountants and information technology experts need to work together to reshape the information ecology rather than relying on images of bombs or planes dropping out of the sky. One area of concern that I discuss in the following paragraphs is a result of poor cybersecurity practices – and legal incomprehension –in IoT devices.

[13] Bruce Baer Arnold and Drew Gough, 'Turing's People: Personhood, Artificial Intelligence and Popular Culture' (2018) 15(1) *Canberra Law Review* 4.

[14] "The analysis of this essay does lead to numerous contrarian ideas. In particular, many features of modern technologies such as "spaghetti code" or "security through obscurity," are almost universally denigrated, as they are substantial contributors to cyber insecurity. Cybersecurity Is Not Very Important, Odlyzko p3

[15] Matthew T. Lee, 'The Ford Pinto Case and the Development of Auto Safety Regulations, 1893—1978' (1998) 27(2) *Business and Economic History* 390.

For clarity, a “Cyber natural Disaster” is something that affects many stakeholders in an information ecosystem rather than merely a few actors. It has a systemic impact. It concerns services that are at the very core of the internet and has a far-reaching effect on entities that rely on them to function, much like cyclone or flood damage to power generation, water treatment and other critical infrastructure has a flow on effect to the well-being of the wider community.

In 2016, Dyn[16] one the major DNS providers suffered a DDoS[17] attack from a botnet[18] army of millions of devices many of which were IoT devices which had been compromised by a piece of malware called Mirari[19]. It found its victims by scanning for devices listening devices based on ARM (a type of low power RISC based CPU used mobile and IoT) architecture, listening on port 23 (telnet) or 2323 (you’re not fooling anyone, thats still telnet.) and then, once found, would attempt to brute force its way onto the system by using a dictionary attack of commonly used usernames and passwords, such as ‘admin/admin’. The result of that insecurity in this instance was that the botnet army of IoT devices compromised with Mirari was able to flood DYN’s servers with approx. 1.2terabits per second.[20]

The Dyn DNS infrastructure not able to withstand this deluge of data and collapsed. The result was wide scale disruption to online businesses and to the users of the services they provided in the US and parts of Europe. All told some 85 different companies (including majpor entities such as Paypal and Netflix) were affected over the course of the attack on Dyn. Although this DDoS attack was directed at only one company, Dyn provides part of the critical infrastructure of the internet. The flow on effect felt across the world was much larger than incapacitation of one single corporate entity. The effect was qualitatively different to the problems we see with defective airbags: The Australian Competition & Consumer Commission for example takes action regarding Takata but we still see traffic on Australian roads, groceries are still delivered to warehouses and children are taken to cricket or the park.

Mirai was so effective because, presumably the manufactures felt that “security through obscurity” was, using Odlyzko’s characterization, a sufficient approach to take when integrating connectivity into the IoT devices. In looking ahead to the 2020 Canberra Law School symposium, what is the harm if your smart toaster or marginally sentient fridge gets hacked? A single compromised toaster or other IoT device on its own is not much of a threat, but when it, and a few hundred million of its brethren are coming at you it is a

[16] S Mansfield-Devine, ‘DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare’ (2016) 11 *Network Security* 7.

[17] J Mirkovic and P Reiher, ‘A taxonomy of DDoS attack and DDoS defense mechanisms’ (2004) 34(2) *ACM SIGCOMM Computer Communication Review* 39-.

[18] M A Fabian, and Monrose Andreas Terzis, ‘My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging’ in *Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets* (2007) 18.

[19] C Kolias, G Kambourakis, A Stavrou and J Voas, ‘DDoS in the IoT: Mirai and other botnets’ (2017) 50(7) *Computer* 80.

[20] M H Syed, E B Fernandez and J Moreno, ‘A misuse Pattern for DDoS in the IoT’ in *Proceedings of the 23rd European Conference on Pattern Languages of Programs* (ACM, 2018) 34.

slightly different dynamic. (We can leave privacy and the physical security of domestic/commercial premises that are reliant on IoT to another time.)

There is predicted to be anywhere between 19 billion and 40 billion IoT devices online in 2019[21], with technologies such as 5G (on occasion promoted by business with perceived close associations with authoritarian governments) already being rolled out across the global.[22] Many of the next generation of these devices set to leverage 5g technologies. Without a serious shift in our thinking about risk, responsibility, regulation and the practice of cyber security we are going to make that much easier for those wishing to do mischief to do so on a much wider scale and with potentially more existential consequences. Law has a role to play beyond criminalisation of that behavior and beyond granting law enforcement additional powers for investigation once harms have occurred

In that environment it is unfortunately simplistic to rely on manufacturers of internet-connected devices to ensure their product meets an undefined minimum level of security. Assuming that we can trust the 'wisdom of the beancounters' on the basis that devices have the ability to be patched when exploits that affect their systems are released is problematic. Cambridge Analytica suggests that trust in protestations about a commitment to good corporate citizenship may simply be too much to hope for. Do we need to rethink consumer law for the IoT Age? The wise lawyer and informed beancounter might disregard complacency and be cautious about adding IoT connectivity to a range of appliances as cheaply as possible if faced with the likelihood of sustained litigation and meaningful penalties because the IoT juicers were used by a state agent or a 19 year old hacker to take down a company's online services for a week. Estonia's experience may be more relevant than what happed in Honolulu in 1941.[23]

Legislation may very well be required to ensure that manufacturers comply with a basic level of security to protect individual devices, their owner and the very critical infrastructure of cyberspace that we take for granted so much these days. A model is provided by 'fit for purpose' under the Australian Consumer Law. In California[24] and in the UK[25] legislation has been passed or is under development which ensure manufacturers meet a basic level of security on their devices.

[21] Adam Thierer and Andrea Castillo O'Sullivan, 'Projecting the growth and economic impact of the internet of things' (George Mason University, Mercatus Center, 2015).

[22] Emily Taylor, 'Who's Afraid of Huawei? Understanding the 5G Security Concerns' Chatham House (9 September 2019) https://www.chathamhouse.org/expert/comment/who-s-afraid-huawei-understanding-5g-security-concerns

[23] Michael Lesk, 'The new front line: Estonia under cyberassault' (2007) 5(4) *IEEE Security & Privacy* 76; Thomas Rid, 'Cyber war will not take place' (2012) 35(1) *Journal of strategic studies* 5; and Mary Ellen O'Connell, 'Cyber security without cyber war' (2012) 17(2) *Journal of Conflict and Security Law* 187.

[24] A D Johnson, M M Lee and S Tronson, 'Public Safety and Protection by Design: Opportunities and Challenges for IoT and Data Science' in *Women Securing the Future with TIPPSS for IoT* (Springer, 2019) 119.

[25] Leonie Tanczer, Irina Brass, Miles Elsden, Madeline Carr and Jason Blackstock, 'The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape' in Ryan Ellis and Vivek Mohan (eds.), *Rewired: Cybersecurity Governance* (Wiley, 2019) 37.

In Australia there seems to be some debate as whether the legislation is explicitly needed, or the market will self-regulate. Regardless of which side of that particular ideological divide you find yourself on, one area that will yield definite results is user education. The idea their smart appliances should have good cyber hygiene practices (and more disquietingly that their personal computer or smart phone needs the same hygiene) is one that many people do not consider. Those consumers enjoy the convince of connected devices but do not engage in effective self management and take responsibility after considering the security ramifications of these devices. That lack of agency becomes even more important from a personal rather than systemic aspect if that smart device wants to capture or store personal information, such as email addresses, passwords and credit card details

I solemnly swear they're up to no good!

Odlyzko contends that cyber criminals are, like their bricks & mortar counterparts, somewhat stupid. Although this is clearly true for a subsection of the criminal element the characterization is too broad and too backward looking for comfort.

Some actors who commits cyber dependent crimes are the equivalent of grifters, con artists or those commiting smash and grab style crimes. For the last 10 to 15 years they are what we have been taught we need to defend ourselves against. We have gotten pretty good at spotting and ignoring those 'I am a Nigerian Prince …' scams. Importantly, just as we have gotten better at dealing with that kind of cyber-crime, some criminals have learnt as well. A salient aspect of the global information infrastructure (readily identifiable services at your fingertips) even the not 'very smart' ones can buy or rent the tools they need to commit crimes. CaaS, or Crime as a Service, allows more sophisticated criminals to build and sell or rent frameworks which others can use to commit cyber dependent crimes. Not having the necessary technical skills is not the impediment it used to be and will not necessarily be solved through official/corporate assembly of very big data sets and artificial intelligence.

It is not just the prevalence of these tool sets but the technical sophistication of the tools being employed. In 2010 a piece of malware known as Stuxnet[26] destroyed the SCADA[27] systems running centrifuges at the Iranian government's nuclear enrichment program. This type of malware is known as an APT or adaptive persistent threat. Malware designed to sit quietly within a target network and collect information and or act when sent a specific trigger.

The traditional school of thought about this type of threat is that it is only able to be executed by state actors. However, recent trends in cybercrime indicate cyber-crime syndicates are gaining access to and actively exploiting these

[26] N Falliere, L O Murchu and E Chien, 'W32. stuxnet dossier' *White paper, Symantec Corp., (2011) 5*(6) *Security Response* 29.

[27] SCADA, ie Supervisory Control and Data Acquisition, is a control system architecture which provides a command and control interface for industrial, water, power, and manufacturing facilities.

kinds threats against organizations that do not have the resources or technical sophistication for identification and defence. These are often small and medium size entities that provide a target rich environment. They are often targeted repeatedly.

In the case of ransomware attacks, Odlyzko is correct in the regard that these criminal entities will often ensure the victims can recover so that they can targeted again, and indeed will be unless they can perform an effective forensic analysis of the previous attack and establish effective defences. This might be outside the capabilities of many smaller organizations.

Recent years have seen WikiLeaks release the Vault 7[28] technologies into the public domain and state actors engaging with cyber-criminal syndicates to carry out acts of cyber espionage on their behalf. Criminal organizations can and will apply these tools and techniques to their own ends. As their attacks evolve, so too much our approach to defending against those threats. FireEye the global security company monitors the top twenty major ATP groups who receive direction and support from nation states.[29] These are examples of sophisticated criminal groups that operate at the direction of, or with support of state actors.

If our general approach to IT security was working as Odlyzko contends, why according to MacAfee's annual security report[30] has there been 118% increase in the number of reported ransomware attacks from Q4 2018 to Q1 2019 and overall holding at about the same levels, quarter to quarter. Similarly, there has been an increase in attacks using the software supply chain.

Odlyzko contends that spaghetti code can used to increase the security of a system.

> They are based on increasing complexity, to enable many of the "speed bumps" that limit what attackers can do and help trace them. Spaghetti code has already been helpful, and can be deployed in more systematic ways. [31]

This might have been true in the days when every single line of code was developed in house, (and even then, there were few things more tortuous than trying to troubleshoot code that had no structure and was not self-documenting.) In 2019, why write a piece a code when I can find a module online that does that exact function I need? I save time and hassle; I can focus on other things.

The salient problem is that author/s of that code has probably used other modules found online to perform a function in their code so they do not have write it, and so on down the line it goes. You have lost control over your

[28] S Shane, M Rosenberg and A W Lehren, 'WikiLeaks releases trove of alleged CIA hacking documents' *New York Times* (New York, 7 May 2017)

[29] https://www.fireeye.com/current-threats/apt-groups.html

[30] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

[31] Code that is unstructured and extremely difficult to support after release, especially by those who did not have a hand in its development.

software, someone may have put a malicious function into a piece code three points away from you on the supply chain and suddenly, your new in hour Payroll system, or new mobile app is compromised from inception. It does not matter how difficult you make understanding of your code, as an inheritance it has got malware baked into it. As a consequence in practice all that reliance on spaghetti code is going to do is to make that much harder for someone to try and figure how the system has been compromised.

There's an App for that, right ?

Odlyzko's positions on several topics are expressed with verve and are not unreasonable. He makes many useful observations on cybersecurity and its role in society today. However, the idea that we just need to keep on keeping on (the policy version of the 'Keep Calm And Carry On' meme) will lead to problems at a systemic rather individual level. Addressing that risk involves asking some hard questions about law and responsibility, particularly in a discourse that brings together information technology experts, legal practitioers, educators and public policymakers.

In this Op Ed I have chosen a brief response to several topics raised by Odlyzko, highlighting that information cultures and technology change, and that a lack of forward thinking will result in substantive harms. To use an Australian idiom, the "She'll be right, mate!" approach is not going to cut it. Technologies like IoT, 5g and deep learning are making our professional and personal lives richer but they also mean that we are arming those wishing to commit crime, espionage or social destabilisation with tools that pose real concerns.

After the Second World War the Japanese developed a customer-oriented zero-defect manufacturing and continuous improvement methodology which means they worked to deliver products to consumers that has a fewer flaws as possible.[32] In today's 'first to market' app driven society where 'Minimum Viable Product' is the socially and legally accepted mantra of many (and where conventional risk allocation means consumers are coopted for fault detection and experience ongoing patching) we seem to have forgotten this thinking. It is to our detriment, given the focus we place on our personal data and privacy. We need to make sure that our approach to cyber security from the technical, legal and educational perspective is a 'boots and braces' approach.

Good security practices should be baked into products, not tacked on at the end. That necessitates thinking about standards and liability, with a forward vision of what might be done through for example the Australian Consumer Law rather than merely through Australia/international criminal law. Just as importantly, education about good practices and processes should be incorporated into the education system as early as possible. This should happen through the course of people's lives and as a basis for strengthening the information economy through consumer empowerment is potentially the most difficult response.

[32] Dean M. Schroeder and Alan G. Robinson, 'America's most successful export to Japan: continuous improvement programs' (1991) 32(3) *MIT Sloan Management Review* 67.

I began by questioning Dr Strangelove's enthusiasm for looking on the bright side of Armageddon (fewer road accidents! No pesky voters! Companionship in the well-equipped executive bunker!) We do not need to embrace Dr Strangelove or the wisdom of the beancounters. Cybersecurity *is* extremely important and can be fostered through imaginative approaches to law reform. Just as important is the need not become complacent in your thinking about where the next threat will come from and how to defend against it.

To borrow from a term I used above, when it comes my own cybersecurity, or my daughters or my parents, we should be asking ourselves are we aware enough to know.... what is the "Minimum Viable Security" I need?

***