Think Ahead

ACCA

Constant Forward Motion:

The evolving phenomenon of cybersecurity regulation and the race to keep up

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants. It offers business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **178,000** members and **455,000** students in **181** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **92** offices and centres and more than **7,110** Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. It believes that accountants bring value to economies in all stages of development and seek to develop capacity in the profession and encourage the adoption of global standards. ACCA's core values are aligned to the needs of employers in all sectors and it ensures that through its range of qualifications, it prepares accountants for business. ACCA seeks to open up the profession to people of all backgrounds and remove artificial barriers, innovating its qualifications and delivery to meet the diverse needs of trainee professionals and their employers. More information is available at: **www.accaglobal.com**

Cybersecurity is the biggest single issue relevant to businesses of all sizes, from micros to multinationals. Its effects go beyond the businesses themselves, affecting customers, business contacts, shareholders and supply chains. As infrastructure, trade and patterns of consumption develop new models that increasingly reflect a new order of cyberspace with ever more tenuous links to conventional geographical and political constraints, so business will inevitably have to adapt itself to the new environment.

Background

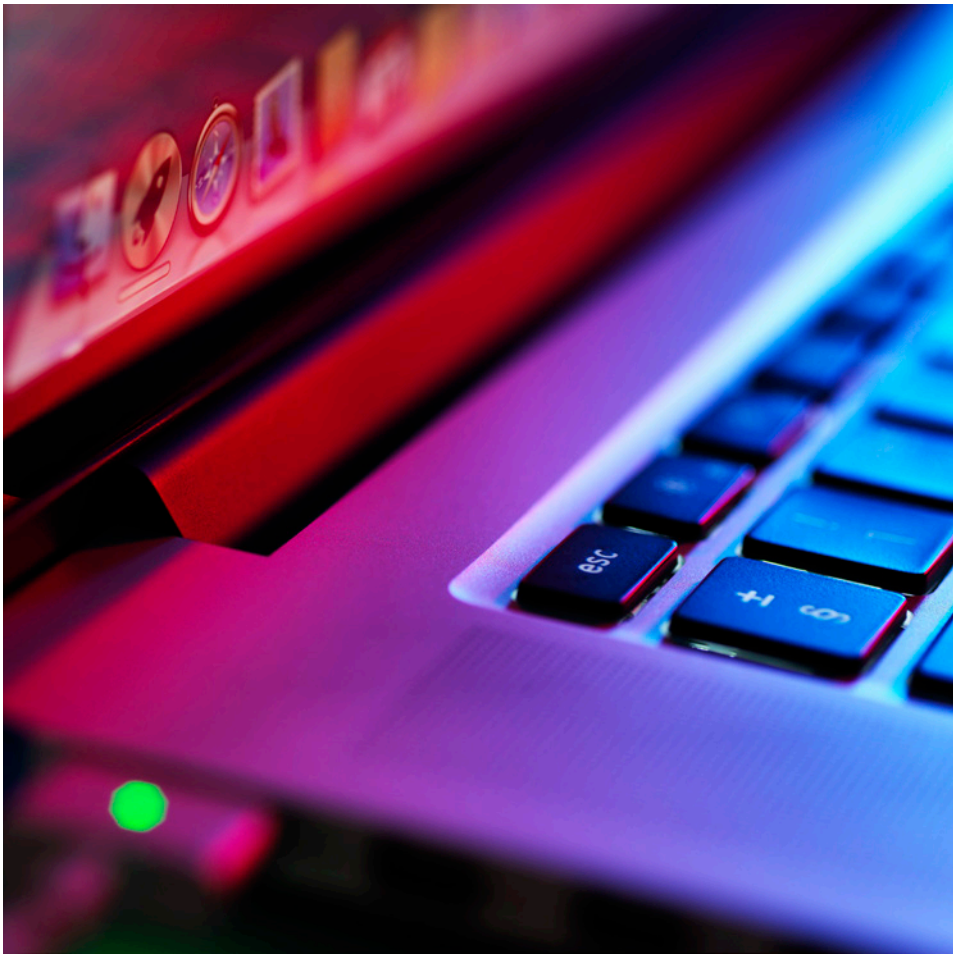
Regulation of business and the activities of those who undertake it is an integral part of modern global society.

Regulation of business and the activities of those who undertake it is an integral part of modern global society. As technology becomes an ever more essential part of doing business, so the constraints of the regulatory framework applicable to that technological capacity will determine the characteristics of a business and its behaviours within society. One of the key themes of ACCA's Global Forum for Business Law is considering what part the law should play in bringing about a more long-termist and 'socially responsible' approach to the running of businesses, an approach that society now seems to demand. The creation and implementation of appropriate regulatory mechanisms will be central in shaping the future of the business world.

Businesses have always depended on the exploitation of knowledge, skills or opportunities that are not available to others. For most enterprises, interaction with the internet and cyberspace does not in itself involve any skill or craftsmanship, but it does allow for knowledge to pass more freely, and can give the opportunity to exploit knowledge that might otherwise not be available. For example, a price comparison website shares knowledge about which retailers are selling a given product; those that have an online presence will have the opportunity to take advantage of the consumers' enhanced access to knowledge.

The use of cyberspace in business is an evolving phenomenon. Some years ago, computers were used simply to store and process information within each business. Each physical machine was isolated, connected to the rest of the business by paper printouts.

Then came networks and the internet, and the ability to move information from one computer to another. Orders could be placed directly into systems – but with that advance came the issue of how to protect the business's computers from unauthorised access. Now things have moved one step further, with data stored increasingly in the Cloud. Maintaining security is no longer a discrete physical operation implemented by the business; security is a commodity purchased from the Cloud providers, a centrally distributed service effectively outsourced to a third party.



This report will explore the scope of cybersecurity as it applies to business, and consider the extent to which a business should seek to protect itself.

Of course, that outsourcing does not absolve the business from its responsibilities, nor mean that it has no input into the effectiveness of its security measures. Rather, the rapid transition from almost entirely physical security measures to those needed for a far more dispersed spectrum of risks highlights the dangers of trying to predict the shape of future business models. The shift from

conventional PINs towards biometrics and other authentication methods is an example of technological change.

This report will explore the scope of cybersecurity as it applies to business, and consider the extent to which a business should seek to protect itself. The report will consider the most effective response mechanisms, and the extent to which adoption of those mechanisms should be mandated by law.

IS THERE A SINGLE CLEAR DEFINITION OF CYBERSECURITY (AND CYBERCRIME)?

Cybersecurity is defined most briefly by the US Committee on National Security Systems as: 'The ability to protect or defend the use of cyberspace from cyberattacks' (CNSS 2010). Cybersecurity, like any security, is about responses to potential threats. A fuller definition, from the US Department of Homeland Security's NICCS Glossary is 'the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation' (NICCS n.d.).

To the extent that they are related to cybercrime, those threats are deliberate and involve a clear intention to shift the balance of wealth (in its broadest sense) between actors. Whether the intention of perpetrators is to enrich themselves, with or without direct cost to the business, or simply to cause loss to the business in some way (for example by a distributed denial of service (DDOS) attack, or defacement of websites) there is a clearly defined relationship between perpetrator and target.

Security in an advanced society

As the online environment evolves, so security takes on a broader meaning.

As the online environment evolves, so security takes on a broader meaning. Just as security for a modern household involves financial and health considerations as much as simple physical protection against burglars, so cybersecurity goes beyond simple defence against crime. It also covers protection against 'natural disasters', keeping the business's information and data secure in the event of misfortune. The 2013 paper *Solar Storm Risk to the North American Electric Grid* published by Lloyds of London (2013), offers an interesting introduction. Maintaining properly updated backups of crucial data and systems may look like no more than good business practice, but may be far more than just a protection against being unable to conduct your own business.

If associates or customers rely upon data that the business holds, or the consequences of that data, a failure to secure the data properly can open up extensive liabilities for consequential loss and damage. The value of the data to, or in the hands of, third parties can expose the holder to the risk of far greater losses than might have been apparent from the value that the data has to its current holder.

The value of the internet lies in its character as a source of information. Some information directly affects the real world (instructions to move money between bank accounts or, increasingly, to switch on the heating half an hour before the householder arrives home) while much of it simply informs other decisions (from big data analysis that predicts purchasing patterns to identity checks whose outcome may authorise a specific money transfer). Much of that information is held by businesses, and used directly by them to implement business transactions. There is a value in this information, to the business, to the customers themselves, and of course to criminals.

Because the information is valuable to the business, it has a self-interest in protecting it, to maintain the commercial advantage it confers. Because the information is valuable to customers and other third-party 'owners', there is a public duty on the business to protect the property of others over which it has custody. And finally, because it has value to thieves, there is an incentive to protect it from theft.

To the extent that a business stands as custodian of the originator's data, there is a social duty upon it to protect it.

PREVENTION IS BETTER THAN CURE

Cybersecurity falls broadly into two parts – preventing attacks and defending against attacks that nevertheless occur. The most comprehensive theft prevention deals with the cause rather than the effect. Apprehending attackers is the role of law enforcement, and the novel nature of the offences allows for a new range of strategies in this regard: either through direct action against individual

perpetrators, or wider actions to disrupt their business model. When it comes to protecting the value of the information to customers and the business itself, the mechanisms and motivations are less clearcut. Within the business itself, the value of information to all parties may not be clearly known – it may have uses to the owners or to criminals that go beyond its use-value to the business. So the criminals' motivation for stealing information, and all the possible outcomes of its loss, may not be clear.. Unlike physical stocks and assets, digital information can be copied and replicated almost infinitely. 'Theft' of information may not deprive the original owner of that information, but can nevertheless compromise its value.

GOOD HYGIENE AIDS PREVENTION

The second aspect of cybersecurity is defence – how should potential targets protect themselves, and what role should the authorities have in ensuring that those defences are effective?

It may at first sight appear that there is little or no justification for legislation requiring a business to operate in its own interests; such behaviour should be the obvious default of any rational decision maker. In practice, the information held by business typically has two values: its value to the business, and its value to the originator of that information.

To the extent that a business stands as custodian of the originator's data, there is a social duty upon it to protect it. In surveys CEOs and CFOs often cite cybersecurity as a risk of growing importance, but it is also widely believed that unless businesses have directly suffered from a cyberattack then advice and guidance, whether issued nationally or supranationally, is likely to fall on deaf ears, as businesses greatly underestimate the likelihood, and likely impact, of cyberattacks.[1]

Moreover, it is often not the largest businesses that are the direct target of criminals. There are many recorded instances of successful attacks against large businesses carried out by gaining access to computer networks operated by smaller suppliers that have privileged access to the purchasing systems of the larger organisation.

If systems are not properly secured and segregated then attackers can use that initial access point to roam the whole of the victim's network, helping themselves to whatever information they desire. This is typically customer credit card details, where these have been stored in accessible form, although increasingly the login details themselves are harvested, as many consumers continue to use identical credentials across multiple sites.

1 http://www.itsecurityguru.org/2015/07/07/uk-small-businesses-in-the-dark-about-cyber-security-with-over-half-not-prepared-for-data-breaches/
http://www.securitymagazine.com/articles/86653-study-says-75-of-us-organizations-are-not-prepared-to-respond-to-cyber-attacks
http://www.computerweekly.com/news/2240238466/Delusion-about-cyber-security-growing-says-Cisco-report

The character of cybersecurity regulation

Cybersecurity is not primarily an issue of dispute resolution, governing legitimate relations between parties.

Cybersecurity is not primarily an issue of dispute resolution, governing legitimate relations between parties (save to the extent that it impinges upon the fallout from cybercrime, although there is, of course, a necessary preliminary of the criminal/malicious act that precedes the 'dispute'). If society can or should regulate to prevent the initial cybercrime, then governance of the consequential disputes inevitably becomes moot.

So, legislators are dealing entirely with a branch of law concerned with restricting undesirable behaviours. This can be done affirmatively, by imposing explicit restrictions on how persons should behave, or 'negatively' by setting out only the punishments that will follow should particular events be allowed to happen, leaving the actors to prevent those outcomes as they see fit. The distinction is between behavioural frameworks and consequential impacts. A parallel is the difference between laws imposing speeding restrictions and offences of dangerous or reckless driving – the former seek to guide outcomes directly while the latter come into play only if certain outcomes are noted.

The world of business and commerce is awash with rules of the former type, governing issues such as business form, transparency and stakeholder accountability. Regulations governing registration and conduct of business are widespread. The function of such rules, which have been developed over centuries, is to safeguard the interests of all parties to commercial transactions.

Technological developments have broadened massively the scope of transactions that need to be governed and the internet is key to much of that growth. Nonetheless, cybersecurity covers far more than just internet transactions. Devices such as skimmers enable criminals to collect and store card information from ATMs, electronic tills and card readers for future use, without any need for direct internet involvement; physical access to a card is all that is required. Likewise, while the bulk of cyberattacks use the internet in some way, typically to feed information back to the perpetrator, physical attacks using keystroke loggers and the like are still common, and can offer distinct advantages for criminals.

Take, for example, attachment of a skimmer via a USB to an electronic till; if the device can be disguised or concealed then it can remain in place for some time, pending later physical collection by the perpetrator. If located before then it will not necessarily offer investigators clues as to the identity of the criminals, or how they can be found. Conversely, any attack that directly uses the internet will leave traces on any number of devices, including third-party servers.

HARD LAW OR SOFT LAW?

There is a tension between the needs of society and the restrictions of different types of regulation. Given the rigidity of formal legislation, can it respond rapidly enough to technological change? Is 'soft law' really appropriate for the consumer protection aspects? As recent developments in USB (in)security have shown, attack vectors that might previously have been considered too complex for widespread use can rapidly become practical for even the least sophisticated of criminals.

The level to which systems are interconnected brings a further new dimension to regulation of cybersecurity risks to business. As the examples of indirect attacks show, there will be a balance between security and utility. If a business is to derive the full benefit from use of technology, then security must be compromised to some extent in order to allow communications with other systems.

AN IMBALANCE OF RESOURCES

The preferred attack vector for criminals will always be the weakest link in the chain, and that may typically be an SME that is less likely than a larger business to have the resources to implement comprehensive security measures. Issues of liability for consequential loss may need to be considered. As between the parties these will typically be covered by existing principles of contract and negligence law, but the question arises whether the public interest is so great as to justify further sanction.

There are already examples from the US of shareholders in a company launching proceedings against the directors for the loss suffered as a consequence of a data breach. Where such a breach has been the result of lapses on the part of a business partner further along the chain there seems no reason in principle why liability should not attach where the fault lies – although of course the question of adequate redress remains, given that typically a smaller, less solvent business will ultimately be responsible for the initial breach.

The role of insurance

The response of business to risk is often to mitigate or insure.

The response of business to risk is often to mitigate or insure. In the case of cybersecurity, however, the scope for insurance might be more limited than it is for established physical risks such as fire or flood. It is in any event a relevant consideration that insurance companies will view their role as mitigating unavoidable or external risks – shouldering business risks is what shareholders are for. If the business has not properly considered and addressed the environment in which it operates and adapted its own processes accordingly, then an insurer will not be the appropriate counterbalance to that risk.

Nonetheless, cybercrime risk insurance is a growing field. The difficulties for the underwriters lie in setting premium levels and calculating the risks. While take-up remains low there will inevitably be a higher loading of premiums, which in turn runs the risk of delaying take-up. More significantly, the underwriters simply do not yet have enough information to assess their exposure accurately. In particular, the issues of aggregation and systemic risk remain worryingly unquantifiable. A single significant cybersecurity incident could easily affect a far wider pool of businesses than would be the case for, say, an extreme weather incident; and while the market can predict the factors which govern a large storm and investors can diversify simply by spreading geographic concentration of risk, an equivalent mechanism has not yet been developed for cyber risks.

Mandatory insurance would almost defeat the object of the exercise, and would certainly be susceptible to the moral hazard argument that typically accompanies the offering of broad insurance cover. It would also force underwriters and brokers far more rapidly into a motor insurance style scenario, but without the available pool of information to set premiums. In any event, cyber insurance in its current form is more similar to business continuity insurance, displaying a far wider variation of quantum and likelihood of risk than for motor policies.

It may well be the case for the time being that the problem is not so much a carelessness on the part of business despite the availability of cover, so much as a failure to realise that the cover is available, or even that the risk exists.

The impact and scope of cyber insurance will itself be moulded by the shape of wider responses to cyber risk. If business is encouraged to protect itself, rather than insure, there is likely to be an inefficient overproduction of protection. Resources will be diverted into redundant protective mechanisms, replicated across every business, when a single shared insurance pool could have freed those resources up for the underlying business. If society's efforts are directed at prevention of cybercrime, by reducing the number of criminals and attacks in the first place, then the individual costs of protection will fall, but there is a corresponding risk of free riders, seeking to benefit from the measures implemented and paid for by society without directly contributing towards them.

The threat within

Very often, it may be the business's own employees and agents who pose the threat to the broader security of the business.

Very often, it may be the business's own employees and agents who pose the threat to the broader security of the business. Whether through deliberate action or simple incompetence, they are likely to be involved more or less directly in every data breach. Where there are sanctions applicable against individuals, the penalties can be severe. Sentences under the UK and US computer misuse legislation can run to 20 years or more per instance.

In many cases, existing data protection legislation is relevant and will incorporate sufficient conditions, safeguards and penalties to provide the desired level of protection for society. Application of such legislation to new models of data holding may involve a degree of judicial interpretation and with it the inevitable costs of litigation and temporary uncertainty. Nevertheless, these costs will undoubtedly be smaller than those of attempting to develop and implement entirely new legal structures to govern the public duties of businesses in relation to the information they hold as custodian for others.

Conclusion

Cybersecurity is a fast moving field. Things change faster than most legislatures could hope to keep up with.

Cybersecurity is a fast moving field. Things change faster than most legislatures could hope to keep up with. Formal statute law becomes outdated. The answer is an appeal to the enlightened self-interest of business to protect itself, combined with a recognition from all involved that existing principles of consumer protection and business regulation can and should be adapted to respond to the new threat.

This does not absolve authorities from any responsibility to act. Governments and other authorities have a role to play in disseminating best practice and guidance. Yet time spent on legislation seeking to punish those who will already suffer through their own foolishness is time wasted when it could be better spent on other mechanisms for tackling the perpetrators. To remain effective, any 'hard law' regulation would need to incorporate elements of a 'state of the art' defence, such as that present in the EU product liability directive. Even then, the problem of updating the law is simply moved down the chain to become a problem of updating defences and practices, effectively introducing a second layer of uncertainty into the analysis of risk.

The most effective use of public funds in tackling the approach of business to cybersecurity is in the raising of knowledge of businesses about the best options for defence and preparedness. Broad guidance aimed at ensuring outcomes, rather than prescriptive regulation governing underlying actions, will offer the required flexibility.

Development of certification and assurance regimes for business, so that stakeholders can be confident that those businesses with which they interact are adequately protected, would be a valuable tool. In practice, the necessary compromises between specificity of regulation and broad applicability will make development of such regimes a difficult task. Supranational guidance would be ideal, but in the first instance a domestic lead taken by key nations in the pattern of international trade would have a rapid 'trickle-down' effect.

As the example of the UK Bribery Act 2010 shows, imposition of ostensibly domestic legislation upon sufficient actors can have a far broader impact, especially where (as with much US financial crime legislation) the legislation is intentionally extraterritorial. A combination of credible assurance and authorisation regimes and the enlightened self-interest of well-educated businesses will offer a more responsive and adaptable model for consumer and business confidence in cybersecurity than would any attempt to create prescriptive legislative standards.

References

CNSS (Committee on National Security Systems) (2010), *National Information Assurance (IA) Glossary* <http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf>, accessed 30 November 2015.

Lloyds of London(2013),'Solar Storm Risk to the North American Electric Grid', <https://www.lloyds.com/news-and-insight/risk-insight/library/natural-environment/solar-storm>, accessed 30 November 2015.

NICCS (National Initiative for Cybersecurity Careers and Studies) (no date), *Explore Terms: A Glossary of Common Cybersecurity Terminology* <https://niccs.us-cert.gov/glossary#letter_c>, accessed 30 November 2015.

EA-CYBERSECURITY-REGULATION

ACCA The Adelphi 1/11 John Adam Street London WC2N 6AU United Kingdom / +44 (0)20 7059 5000 / www.accaglobal.com