Cyber-Storm

A future system-wide hack could travel at light speed, faster than news of its occurrence, leaving nothing but silence, puzzlement and a slowly dawning fear in its wake.

Mark Johnson, The Risk Management Group

Risk is fractal. It cascades down from the massive server farms of Google, Amazon and Facebook, down through the cables and platforms of the internet service providers and telephony networks, on downwards through the online retailers, the banks and insurers, the government agencies, into increasingly 'smart' offices and homes, across desktops, laptops, tablets and smartphones, into every app, email, text, selfie, Like and link. Risk is there at every level and inall its forms, infinite in its capacity to devastate lives and livelihoods, to shatter reputations, to destroy relationships and expose the vulnerable to images and ideas they are not able to assimilate without suffering psychological harm. Today's technology risks are viral, ubiquitous, multi-faceted, globalised, virtual and potentially instantaneous. A future system-wide hack could travel at light speed, faster than the news of its occurrence, leaving nothing but silence, puzzlement and a slowly dawning fear in its wake.

The diffusion of personal data

We are now witness to an ever-wider dispersion and diffusion of identifiable sensitive personal and financial data. We are moving from customer segments of many towards segments of one, in which social media and big data firms understand the inner life of each user better than the user'sfamily and friends. With society's almost total dependency on information technology, with billions of new digital touch points emerging via the Internet of Things, with converging communications, cloud storage, Apps, and artificially intelligent systems, allcomplimented in some cases by potentially disruptive and largely unregulated new payment models, we are either poised to launch into a brave new world, or to dive into the perfect storm; the Cyber-Storm.

WannaWeep?

The widely reported WannaCry attack in May 2017 affected more than just the NHS. WannaCry encrypted an estimated 200,000 computers in 150 countries. It was an example of a Worm; a clever bit of malware that spreads autonomously, stays hidden for a period, and then launches itself on a pre-determined date.

What does the CyberStorm look like? It looks like WannaCry but on a much larger scale. It might take the form of a Worm hidden in a viral file widely shared via Facebook, Dropbox and email. It stays hidden for months as its spread continues across the global Internet, exploiting previously unknown chip vulnerabilities affecting a wide range of systems.

When it finally activates itself, early on a Monday morning, WannaWeep affects one billion machines of all kinds, and takes out the Internet in a sudden cascading series of failures. The spread of this infection only fifty times wider than WannaCry, but its impact is thousands of times greater.It has attained critical mass.

As we head out for lunch that Monday, we see long queues at the cash machines. The people at the head of each queue are clearly annoyed about something. Small knots of people are arguing. Those further back in the line are peering apprehensively at the excitement ahead. One man is counting the residual cash in his wallet.

More lines are forming outside bank branches and our credit cards don't work when we attempt to pay for our takeaway meal. Costa and Starbucks already have hastily penned 'Cash Only' signs in their windows. A quick check reveals that our mobile Internet access has vanished; no payments via our banking apps are possible. Cash registers won't accept Apple Pay. The mobile network is jammed and out laptops can't logon to WiFi. At a nearby intersection, a driverless lorry stands motionless, blocking the flow of traffic.

Back at work, now feeling distinctly peckish, there is still no Internet service. The financial and communications systems have all come to a standstill. The Internet has gone down and,though we have no way of knowing this, it will stay down for several weeks. We start a

long trek home on foot because public transport isn't running. The more cynical among us are already mentally toting up the cans of beans and sardines, bags of rice and pasta, and the quantities of olive oil in our kitchen cupboards; just in case. Just as a sensible backup. Perhaps the local supermarket will accept an IOU? What do I have in the garage that can serve as fuel for my barbeque? I'd better fill the bath and any containers I can find as soon as I get home!

The challenge of AI

Let's assume the Internet stays up for the time being. Advances in 'Narrow' AI decision-making, along with new operating models such as Open Banking whereby regulated third parties will be permitted to seek consent from their customers to access individual customers' banking records to support such decision-making, only serve to fragment the risk model into ever smaller parts as sensitive data is distributed ever more widely while our dependency on machine learning grows in parallel. Computer-based decision-making also gives rise to new targets for hackers and fraudsters; why steal data when you can potentially take over the entire decisioning process of an organisation,potentially altering decisions on lending, borrowing, investing, rewarding and awarding, marketing, pricing, trading, or the ordering, production and distribution of high-value physical assets? After all, turning 'Computer says No' into 'Computer says Yes!' will always qualify as the ultimate hack.

The problem with SMEs

The President of Russia governs a state blessed with a sophisticated, deeply suspicious and highly experienced security apparatus. It is an apparatus that possesses extensive knowledge of internet security vulnerabilities and possible exploits, and which has its origins in the Tsarist and Soviet regimes that governed the vast landmass of Russia and her satellites for many lifetimes.

Yet, despite this ingrained security mindset and a long history of respect for secrecy, the President's private financial records still found their way onto the public internet where

they have since been subjected to intense scrutiny by the world's media. And Mr Putin was only one of thousands of high-profilepeople to suffer this affront.

The reason for this comedy of errors was very simple. The people affected, or their aides, had sent this confidential information to an obscure Panamanian law firm that specialises in tax matters. The firm might be expert in tax reduction, but it turned out be inept at managing information security. With outdated systems boastingmore than 25 known security vulnerabilities, it was inevitablyhacked, and the records exposed.

This is a repeating pattern in which large, highly secure organisations share sensitive data with smaller, less advanced, less secure ones. As the data cascades down, with the medium-sized firms passing data on to even smaller sub-contractors and individual consultants,for processing, analysis and advice, the risks cascade down too, growing larger as the data custodians grow smaller. Before you can say 'Bolshoe spasibo!', the most sensitive of secrets sit on the laptops and tablets of uncounted thousands of unaudited and insecure third parties. Anyone engaging in Open Banking should urgently familiarise themselves with this picture.

Regional responses to a global problem

There is a real dichotomy between this accelerating distribution of data into the hands of growing numbers of third parties and the core principles of data protection regulation, as reinforced this year by the new EU General Data Protection Regulation or GDPR. This conflict is worsened by the fragmented nature of the regulatory environment and the lack of centralised global oversight in the face of a globalised threat affecting globalised infrastructure. Unless we can impose a common set of standards on providers and ensure compliance worldwide, we are unlikely ever to win the cyber-security struggle.

And it is a struggle. Only this week, we are being warned by no less than the UK's Chief of the General Staff, General(Sir) Nick Carter, that those who wish us ill are rapidly laying the groundwork for massive cyber-attacks against various parts of our critical national infrastructure. This will incude financial services, the mainstay of our economy and a prime

target. With only a few days' worth of food stocks in our automated, just-in-time-delivery supply chain, a major cyber-storm is the very last thing we can afford. A joined-up approach is long overdue.

Concerns about national legislative efforts

I have an even moresceptical view when it comes to national efforts to legislate for cybercrime risks. I find it difficult to see how national legislative initiatives can effectively address a globalised set of challenges.

Secondly, while I believe that internet and device technology and service providers should be doing more to protect consumers and businesses, I am less sure about the current focus on penalising data custodians. Custodians do not design the technical platforms they purchase from suppliers and many of the vulnerabilities that lead to data breaches are beyond the capacity of most custodians to address or even comprehend.

The recent series of WannaCry attacks worldwidefollowed the exposure of the NSA's hacking toolkit by The Shadow Brokers hacking group. Here we saw a situation in which the NSA not only failed to secure its own hacking arsenal but had earlierchosen not to inform the affected technology suppliers about the vulnerabilities it had identified in their systems. How can it be fair or reasonable for a national government to penalise a data custodian who falls victim to an attack that has its roots in this scenario?

What we are doing today is the equivalent of fining smokers for contracting lung cancer. Yes, smokers are warned about the risks yet choose to continue smoking, but they did not choose to become addicted to cigarettes. Nor did they create and maintain a global market for a flawed product. As with the tobacco industry, it is the internet and device sectors that should cover the cost of their collective failure to adequately protect consumers, businesses and the public sector. Custodians should only be punished when gross negligence on their part is an important contributing factor.

Aten-point plan for regulators

Even with GDPR on the immediate horizon, regulation addressing cyber-security is not yet fit for purpose. We don't need to be particularly technical to come up with some common-sense rules that regulators worldwide should implement. While these won't stop the more sophisticated hacker, they will help to put a lid on the complete free-for-all we see on todays' internet.

1. **Create benchmarks for device, app and browser security**. Anyone who has attempted to make themselves secure online by adapting their Facebook, LinkedIn or browser settings will have faced an almost overwhelming number of choices, with no guidance offered by the providers as to which are the most effective. Regulators should define baseline security standards and enforce them everywhere.
2. **Opt-out not opt-in to security**. Once security benchmarks have been defined, they must be applied as the default setting in any device, app or service being offered for sale in any regulated market. Users should have to opt-out of security by providing explicit acceptance of the resulting risks, rather than having to search for the relevant settings and then opt-in.
3. **Social networking authentication**. None of us wants to share our social media feed with fakes. We should be given the option to validate our identities with service providers, to receive a green tick from the provider beside our profile picture.
4. **Blocking unauthenticated contacts**. Once authenticated, every social media user should be able to un-friend and block all unauthenticated users with a single click.
5. **Full disk encryption at point of sale**. Disk encryption must be mandatory – no more data theft from laptops left on the train. In this scenario, law enforcement and device manufacturers can still collaborate to unlock devices when justified, but consumers and businesses are better protected from criminals.
6. **Free anti-malware on every device at point of sale.** The installation of anti-malware software must not be an option at point of sale for which the consumer must pay a premium. Anti-malware software is our digital seatbelt. It should be a legal requirement for every manufacturer to install it at the factory and for it to be constantly updated free of charge for the lifetime of the product.

7. **Mandatory software updates for consumers**. Many successful cyber attacks exploit failures by users to update (patch) their systems and software. Automatic updating should be a default setting from which users need to opt-out. When opting out, explicit acceptance of the resulting risks must be given, meaning that victims who opted out of automatic updating cannot make compensation claims when attackers exploit known, unpatched vulnerabilities.
8. **Search engine purging**. Search engine providers must purge their databases of sensitive personal and financial data, such as email lists and password hashes; they must comply with the spirit of data protection and privacy laws. They must also find and remove links to illicit sites providing hacking tools, malware app development downloads or similar services.
9. **Regulation of penetration testing**. A global register of qualified and licensed penetration testers and testing services, working to defined standards, must be established. Only qualified, registered testers should be permitted to offer or provide such services. Unregulated testing should be subject to sanction and any person or business using an unregulated tester should be penalised.
10. **Regulation of crypto-currency markets**. Payment mechanisms such as Bitcoin, a store of value and a medium of exchange, must be regulated in line with any other financial service. Anonymous accounts should be banned and provisions for tax reporting, suspicious transaction alerting, know-your-customer, customer due diligence, PEP checks and the detection of sanctions bypass should all be put in place by providers and transaction handlers.

This list of actions is merely a starting point, a list of key targets. Many will object by saying that most of these targets will never be achieved, but if you nevertheless agree that the targets make sense in principle, then you have defined the underlying problem. Until we adopt and enforce common-sense regulatory controls on a worldwide basis, our entire globalised economic system faces a potentially catastrophic risk; the risk of a Cyber Storm. And this is not a risk we should be willing to live with.