HIGH WIRE:
THE CYBERSECURITY BALANCING ACT
Cybersecurity leaders are walking on a wire. The mass of sensitive data that Technology, Risk and Big Data professionals have to navigate every day has turned the function into a careful balancing act, and the stakes continue to rise. A growing awareness of data as a business-enabler has been shadowed by an increase in the number and complexity of cyber attacks. Each step forwards is a risky manoeuvre. One frayed cable, one breach—and you’ve gone from Cirque du Soleil to six months in a cast.

This white paper looks at the perils and pay-offs on either side of the cybersecurity balancing act. It examines a variety of structural, systems and cultural approaches to the function throughout a range of industries including the military and large energy networks. Our insight is based off a broad research platform and direct interaction with cybersecurity professionals every day. There isn’t a cure-all for cybersecurity yet. But the better functions share some common elements. Without these as a safety net, that high wire starts to look a whole lot shakier.

According to Symantec’s annual Internet Security Threat Report, 2015 saw 430 million new unique pieces of email malware, 9 major breaches with over 10 million identities exposed, and a huge increase in mobile attacks following the platform’s ascendancy and the growth of omni-channel.

It listed over 500 new mobile vulnerabilities (up 214 percent on the previous year) as well as nearly 4000 new Android malware variants (an increase of 77 percent). The report also showed that cyber criminals are discriminating far less between large and small companies, with attacks like the ‘Tech Support’ scam becoming increasingly popular (where scammers call under the pretext of detecting a computer issue and then convince call-handlers to give out vital information).

In the wake of several notable and disastrous leaks in recent months, figures like this are no surprise. The UK’s Defence Secretary Michael Fallon has ramped up the country’s efforts to tackle cyber crime with a proposed £1.9 billion investment over the next five years. Three Wall Street banks are expected to spend $1.5 billion dollars on cyber security in 2016 alone. Banks, governments, film companies and consumer websites have all come under fire. Executive teams in every sector with digitised operations have had a rude awakening as to just what can go wrong when cybersecurity isn’t prioritised.
A growing concern in an environment like this is that companies keep their hard-won data under lockdown, limiting its application as a business-enabler.

A source of ours in a top pharmaceuticals company described the situation as being like having a bank vault when you actually need a wallet: somewhere that data can be readily accessed in a way that’s both mobile and secure. But the problem here is that thieves won’t need a safe-cracker to get your information now – they can just mug you. This is the recurring conflict in the cybersecurity space: security and compliance versus access and business-enablement. Companies looking to integrate and upgrade multiple legacy systems are wary of exposing themselves. Structural uncertainty as the function evolves can stifle data-driven innovation while leaders figure out how best to use information.

Function restructure activity is particularly buoyant at the moment in fact; with the optimum setup being a fully-secure unit that isn’t insulated from the wider business’ needs (and vice versa). But where hazards exist, opportunity persists. From a talent perspective, many of the cybersecurity professionals we spoke with were excited by the prospect of leading restructuring efforts in functions that weren’t yet fit for purpose.

The opportunity to rebuild a function has become an enticing proposition in a field that’s both starved for talent and yet bloated by increasing regulatory pressure. The EU’s General Data Protection Regulation, for example, which comes into force in May 2018, is likely to make things even more tedious for UK firms trying to access and transmit data across the common market’s new boundaries in the wake of the Brexit.
building the safety net

ALIGNMENT & STRUCTURE

With the stakes so high, tumbles are inevitable. It’s the position of the net and the strength of the weave that’ll break your fall. But the question of how and where cybersecurity should sit gives rise to a number of related concerns. Which business unit does it sit under? How much autonomy should the function have? Who should be in charge?

We’ve tended to find that a fully autonomous function works well in sectors that handle a vast amount of sensitive consumer data, like Retail.

In these organisations the security, risk and privacy functions are generally well established, with large teams that understand specific responsibilities. But while this is considered a ‘mature’ cybersecurity model in many, issues crop up where the function is a solely Technology-oriented one. Although the systems knowledge here will be exceptional, understanding of wider business needs can suffer. More and more, we’re seeing the cybersecurity platform shift towards a Risk or Business Development capacity in pursuit of a balance between business needs and systems expertise.

As for autonomy, there are two distinct ends to the spectrum. At one end, organisations will occasionally give the security function absolute autonomy. In such scenarios, the function head often reports into the COO or CFO, has their own budget, and is distinct from other departments. But for businesses handling less consumer-centric data, there’s a tendency to be less risk-averse. Cybersecurity leaders here are often given a wider remit of responsibility along with smaller teams, and a heavier reliance on partnering with the wider business. In these instances the function’s autonomy is lessened, but knowledge of operating and information systems should still be firmly integrated among the team; the balance can’t tip too far towards the needs of the business at the cost of secure information.

Alignment is also closely tied into how centralised the function is. A top investment bank we investigated, for example, splits the function entirely among its business units, choosing a fully-decentralised model with figureheads sitting at the Group level. By contrast, others centralise the theme completely, opting for a fully-automated system across all business lines. This also raises the question of whether to structure the function along these lines or do so by geographic remit instead and, again, it depends on your needs. A top American bank has constructed an interesting hybrid model that somewhat balances between the two: US operations are managed by a number of small specialised teams that report into a Group-level Information Security officer, whilst outside the States, regional heads oversee security across EMEA.

However, sources within the bank have spoken of infighting because people are confused as to who ultimately holds responsibility outside the US headquarters. There have also been divisions between the extremely tech-focused specialists in the States and the more broadly BD-oriented professionals abroad. The lesson? Highly-specialised hybrid models can be tripped up if there aren’t clear lines of reporting and responsibility communicated from the outset. A mishap due to infighting can jeopardise the unity of cybersecurity across the entire business.
This theme of unification spans the entire length of the cyber highwire. Your people aren’t communicating? Wobble. You don’t have a defined cybersecurity culture? Wobble. Your systems are incompatible? Audience gasps. Systems, in particular, present a huge challenge to businesses that want to tap into the growth potential of their data without compromising security in the process.

Take the US Department of Energy, for example, responsible for the mammoth task of coordinating the American power grid. A network of computers, field platforms and extensive communications networks pumps out valuable data that can be analysed to enhance the reliability and resilience of the grid itself, as well as maximising energy efficiency nationwide. The DoE have worked for years to facilitate both the security and value of their data, developing what they call the ‘Smarter Grid’: a network that can survive a cyber-incident while sustaining critical energy delivery functions countrywide. Key takeaways from their approach to future-proofing cybersecurity include:

1. UNDERSTANDING YOUR NETWORK & THE THREATS POSED TO IT
The US grid is in part comprised of decades-old legacy devices with limited communication and processing power, many of which are located in unmanned or remote locations. Hackers have tried to capitalise on this by sending malicious commands designed to mimic the actual data these systems transmit, causing malfunctions.

From a cybersecurity perspective, modelling the physical results of such commands can help operators to assess risk well in advance and draw up protocols accordingly.

Besides creating attack scenarios, you don’t have to alter the system itself to improve organisational responsiveness. Simply understanding what you’re currently working with can go a long way to being prepared in the event of an attack. Document network architecture, identify any systems that are business-critical or contain the most sensitive data, and you’ll have a better chance of understanding the risks facing your digitised infrastructure.

2. HAVE A BACKUP
A key example the DoE give is the GPS system used to synchronise devices that measure electrical pulses across the grid. This process allows for real-time monitoring of multiple remote points at once, providing unprecedented visibility over a huge operating area at any time. The department found that these GPS signals can be jammed or ‘spoofed’, resulting in interference or even direct manipulation. They tackled the issue by implementing multiple receivers that cross-check each other as a backup. Don’t rely on one device if it’s handling business-critical information.

Back up your data and investigate if your system has any kind of fail-safe. Symantec’s study found that over a third of the small businesses profiled wouldn’t be able to recover their data in the event of a catastrophic breach. To paraphrase one of our sources in Big Data, ‘don’t allow a small error to become the info-pocalypse’.

3. BUILD CYBER INTO THE FOUNDATION OF NEW INNOVATIONS.
The DoE, in partnership with a number of its distributors, has outlined requirements to ensure that cybersecurity underlines growth from the outset. As we mentioned above, these include the importance of effective management, monitoring, and forecasting as primary aims, but they also highlight more specific challenges.

At times where the business needs are in direct conflict with security objectives, for instance, a balanced approach would require that more risk evaluation takes place during solution selection, implementation, and post-deployment. They also point out that cybersecurity starts at the beginning of a system’s implementation journey, in the supply chain itself. Components can be damaged or directly tampered with and common sense dictates that the more critical a device, the more care needs to be taken to ensure its safe delivery.

If you’re ordering microprocessors for an Apache helicopter, you want a third-party supply chain specialist to handle the logistics.

The DoE also propose a move towards standards-based vendor acceptance. Make sure that different solutions can function in unison without compromising one another, and ask your vendors if they’re aware of any back doors into their systems. Working closely with suppliers can fortify the integrity of your security infrastructure from the get-go. They should understand your needs and be able to review their software or firmware in response to any issues as they arise.

“Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight; whoever is second in the field and has to hasten to battle will arrive exhausted”

SUN TZU, THE ART OF WAR
acrobats

PEOPLE & CYBERSECURITY

So you’ve built the Big Top, put up your safety net – now what? Train your acrobats. Some of the worst leaks in recent memory have been the result of basic human error – like failing to dual-authenticate social media accounts or leaving laptops on a train. Simple errors like this have cost companies and governments millions, not to mention the incalculable damages caused to reputations.

Yet amazingly, when asked ‘who is most responsible for ensuring strong cybersecurity’ in a report published by Cisco last year, individual employees came out last with a vote of only four percent (CEO/Board members were the highest at 39% - followed by the CRO at 35% and CISO at 30%). Understandably, it’s up to C-Suite to make those critical final decisions on how to implement strategy and resources. But the cybersecurity threat has proven time and again to pervade every tier of an organisation. Realising your cybersecurity potential therefore involves the promotion of a culture of training and education, openness, and strong leadership among your employees.

With IT so widespread and a huge proportion of the workforce now on smart phones, privacy and security is an individual concern as much as it is a business concern.

In a forensic study of the cyber-environment in the US military, for example, the Harvard Business Review showed how the largest navy in the world puts their people at the epicentre of their cybersecurity efforts. High-reliability organizations like this, HBR writes, ‘possess a deep awareness of their own vulnerabilities, are profoundly committed to proven operational principles and high standards, clearly articulate accountability, and vigilantly probe for sources of failure.’ Underpinning this stringency is a code of ethics that’s inculcated in all personnel from day one, based on the following operating principles:

1. Integrity
2. Depth of knowledge
3. Procedural compliance
4. Forceful backup and constant oversight
5. A questioning attitude
6. Formality of communication

In this environment, the training and oversight of the individual informs the resilience of the whole. Even simple things like password controls and attachment awareness can reduce the risk of breaches caused by an individual. HP’s Most Effective Security Technologies & Practices 2016 report suggested that 33% of organisations didn’t enforce strong password policies. Simply making employees aware of the risks and promoting diligence is an effective first-line defence. The ‘more eyes on’ attitude of the US Navy (point four), for example, ensures that slip-ups get caught early. They expect mistakes to be reported immediately before they cause further problems. But importantly, they create an environment where employees feel comfortable doing so.

Many of our sources, in fact, stated that the best cyber environments were markedly people-centric, emphasising accountability and trust instead of using restricting and preventative controls. Formal regimentation of procedure doesn’t have to mean constantly living in fear of making mistakes: it means that people are properly equipped with the tools and support they need to reduce the likelihood of those mistakes from occurring and are able to deal with them when they do.

“Unified architecture and state-of-the-art technology are only part of the answer. In nearly all penetrations on the .mil network, people have been the weak link.”

HARVARD BUSINESS REVIEW
The popularity of monikers like the ‘Cyberdefender’ (HBR) and the ‘Secure Digitizer’ (Cisco) are beginning to suggest a new rhetoric of proactivity within the function. ‘Cyberdefenders’, say HBR, ‘need to create “high-reliability organisations” – by building an exceptional culture of high performance that consistently minimizes risk.’

A synergy is beginning to emerge between a defensive technology-based view of cybersecurity and the enabling potential of data. Cisco explains that the Secure Digitizer is someone who takes ownership of cybersecurity by choosing projects with a high opportunity-to-risk ratio – and not just a low-risk profile. Analytics, IoT and Cloud Computing all require a new sensibility.

As digital technologies become more integrated into business functions, so-called Secure Digitizers ensure that all digital processes are re-engineered ‘with cybersecurity as the foundation’.

Innovation, confidence and responsibility have thus become three core traits of the new cyber ringleaders. These professionals develop a strong individual focus on responsibility for data security and encourage an open and innovative environment. For them, cybersecurity underpins the foundation of their work, and the very best will actively promote this same mentality within the wider business.

In many ways, the military’s operating model is both the most relevant to the cybersecurity theme and also one of its most appropriate metaphors. The constant barrage of threats directed at these incredibly tactical systems dramatises the cybersecurity problem in its most extreme form. It also plays on the old adage that ‘attack is the best form of defence’, which – while it doesn’t translate directly – does point to an emerging mindset in the current battle for cybersecurity balance.
In the context of increasing attacks, talent scarcity, an explosion of new applications and mounting regulatory pressure, cybersecurity will continue to be a key priority for executive teams worldwide. Through our ongoing discussion with leaders in the field of cybersecurity, as well as our broad approach to researching the problems that face digitised industries today, we’ve summarised the following attributes of the well-balanced cybersecurity function:
Wilbury Stratton is the leading international executive intelligence firm. Over a third of the FTSE
100 rely on the information we provide to make informed decisions on the strategic direction
of their business. Whether understanding their competitive landscape and the talent that lies
within, mitigating leadership risk or benchmarking their own people, we provide relevant and
actionable information to organisations that transcends geographies, functions and industries.

For a confidential discussion about your requirement please call
+44 (0) 203 727 3333 or visit www.wilburystratton.com