RENAIX

A Guide to IT Audit and Cyber Security

Contents

Introduction

Digital threats to corporations, governments and individuals are at the highest level that they have ever been. Cyber security is not just dominating the headlines but conversations in boardrooms as well. A data leak or similar attack poses massive financial, reputational and legal risks for companies. Smaller companies are even more vulnerable as they might not have dedicated people or resources trying to combat hackers who are actively attempting to target them.

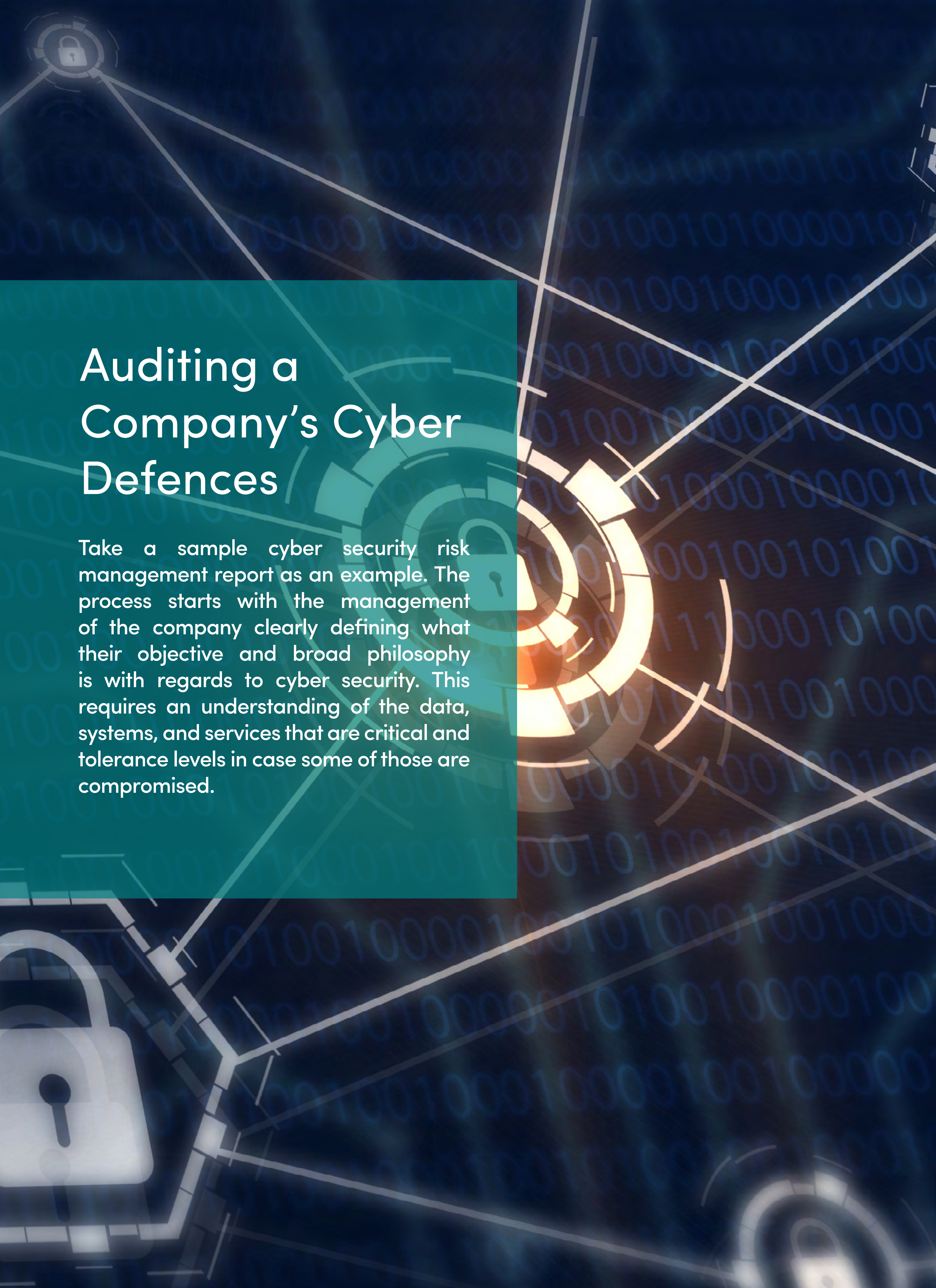
With this in mind, organisations are making efforts to establish cyber security risk management reporting tools. Although existing cyber security tools are not overly sophisticated, some organisations like the AICPA have already begun directing efforts towards this goal. Because of the work public accounting firms already do for their clients, they are in a prime position to offer advice and services related to cyber security. In fact, almost 40% of the leading cyber security consultants are public accounting firms.

Here at Renaix, our team is built around specialisation and market awareness, with 20 years working in the international finance and accounting industry. Our consultants are experts in their field and are at the forefront of innovation in recruitment processes and the latest industry trends. We are therefore well positioned to assist you with any skills or qualifications related questions or concerns you may have.

Feel free to send us your CV and a member of our team will be in contact to offer their consultancy and advice on your options and how to successfully secure your next role. As part of our service, we are also happy to review your CV and provide comments and advice on how this may be improved to increase your chances of landing your next role.

Get in touch now at info@renaix.com, give us a call on +44 (0)20 7553 6320 and join our LinkedIn group for the latest news, trends and open recruitment positions at: www.linkedin.com/company/renaix

If you enjoy this guide, please look out for the next one!



Auditing a Company's Cyber Defences

Take a sample cyber security risk management report as an example. The process starts with the management of the company clearly defining what their objective and broad philosophy is with regards to cyber security. This requires an understanding of the data, systems, and services that are critical and tolerance levels in case some of those are compromised.

The second part is a more exhaustive description of how the company aims to achieve its stated cyber risk management objectives. This requires creating and defining a governance structure for risk management. From therein, the company can take a variety of routes to create a framework that meets their specific criteria. Processes, resources, IT infrastructure, communication channels, review criteria, accountability, environmental factors, scenario testing, etc. are defined to a granular level.

The auditor's role is to then asses the strength of this cyber security plan. Firstly, they must asses whether the strategy employed by the company is in line with their broader principles for cyber defence. Then, they must drill down to see whether each specific component of the cyber security risk management program would be able to successfully fulfill its intended purpose.

Why do you need an auditor for cyber security?

Some have questioned whether it is necessary or ideal for an auditing professional to address challenges related to cyber security preparedness. However, there is a reason why 40% of the top cyber security consultants are accounting firms. It is because they bring to the table multidisciplinary expertise along with the independence and objectivity required to test the limits of a company's defences. Furthermore, the professional and ethical standards which auditors are subjected to in various jurisdictions, along with a requirement for continuous learning, place them in the ideal position to embark on these security audits.

In reality, cyber security risk is just another relatively newer addition to the long list of challenges that companies have had to face over the years. Businesses rely on internal and external auditors to objectively inform them where weaknesses lie or where mistakes have been made. It is these audits and the corrective actions that they lead to, that protect businesses from unseen risks.

Do You Make These Eight Common Cyber Security And Data Risk Mistakes?

According to PwC's 2018 Global Economic Crime and Fraud Survey, about half of all organisations across the globe have reported being a victim of fraud or of some sort of economic crime. Cyber crime figures are near the top of the list with 31% of all organisations being affected. What makes these instances of cyber-attacks even more alarming is the rapidity with which they have been increasing over the years. In this article, we look at the 8 biggest cyber and data security risks faced by corporations in 2018:

Reactive attitude

Rather than actively seeking out vulnerabilities, most companies react only after the damage has already been done. The problem with this strategy is that cyber threats are rapidly evolving and protecting yourself from a type of attack that was prevalent last year will not offer much protection form the latest vulnerability.

Lack of a proper cyber security and data protection policy

Whilst many large companies do have a cyber and data security policy, the implementation is usually haphazard with employees lacking proper training. Additionally, the threats evolve so quickly that most policies cannot usually keep up with them.

Legacy systems

Dated physical infrastructure and old software can be a significant vulnerability. The financial cost of updating systems can be large but the cost of a breach has been increasing exponentially as well.

The human factor

The biggest single risk factor continues to be the human element. As per the PwC report, about half of all frauds were perpetrated by people inside the organisation. Cyber and data security is not only about protecting from outside attack but also protecting against privilege abuse and insider manipulation.

The internet of things

IoT refers to the billions of small connected devices that we see all around us such as internet routers, photocopiers and even smart TVs. These are increasingly being targeted by malicious actors as they often do not receive security updates as frequently as computers and laptops. Any breaches are also harder to detect or isolate.

Bring your own device

BYOD is popular with employees and offers cost savings for companies, however, it puts heavy stress on security infrastructure. It is harder to protect the system when there are thousands of diverse types of devices running different operating systems and security patches. About 70% of all companies believe that data breach is a significant risk with BYOD whilst about 50% are concerned about malware.

Training

The issue of inadequate training comes up at almost every cyber security discussion. The challenge here is the rapid pace of technological advancement which means that training materials need to be refreshed on an ongoing basis and then disseminated.

No recovery plans

It is said that no battle plan survives first contact with the enemy. However, having a proper strategy for recovery, backup and damage control can ensure that the losses from a cyber-attack or data breach are not catastrophic. Whilst it costs more to have redundant systems that are not used 99.99% of the time, they can still prove their worth in the event of an emergency.

These are some of the most common vulnerabilities for companies which are facing increasingly sophisticated and damaging cyber-attacks. The first step for a company to counter this is to create a comprehensive cyber security policy that assesses the risk, mitigates it, monitors it and puts recovery mechanisms in place. We shall discuss the key elements of such a comprehensive cyber security policy in future articles.

5 Simple Steps To An Effective Cyber Security Policy (Part 1)

Cyber security is often cited to be the biggest threat faced by businesses and governments today. A population and economy that is connected globally has its advantages, but it also means that the threats can come from anywhere. Often, it is not possible to stop the threat at the source itself and all you can do is build up defences to protect your business data and information.

Most large companies and governments are already well aware of these threats and they have been spending billions to set up defences like security policies and contingency plans. This has meant that the threat has now shifted somewhat towards smaller businesses who do not have the financial resources to put up a similar level of protection.

However, protection is not just a matter of spending on hardware, software or manpower. The first step would be to set up a robust cyber security policy. Considering that more than half of all breaches happen due to internal human error, this alone can make a significant impact. So, what goes into building a watertight cyber security policy? Let's find out.

Cyber security is a business issue, not just a technical one

Many companies treat cyber security as something confined to the tech department. However, the threats from cyber security are now equivalent to the threats faced by competing products or firms. Even if the company has no highly valuable proprietary data or intellectual property, a cyber breach can still pose a massive reputational risk. Therefore, cyber security should be treated as a priority at all levels of management and by all departments.

Protecting what's valuable

The most valuable assets for companies might not necessarily be physically expensive items but might be data that is residing online in some cloud server. Figuring out what's valuable is the first step to creating a protection plan. And the methods to measure the value of a company's assets must be in line with customer expectations in the 21st century.

Managing weak links

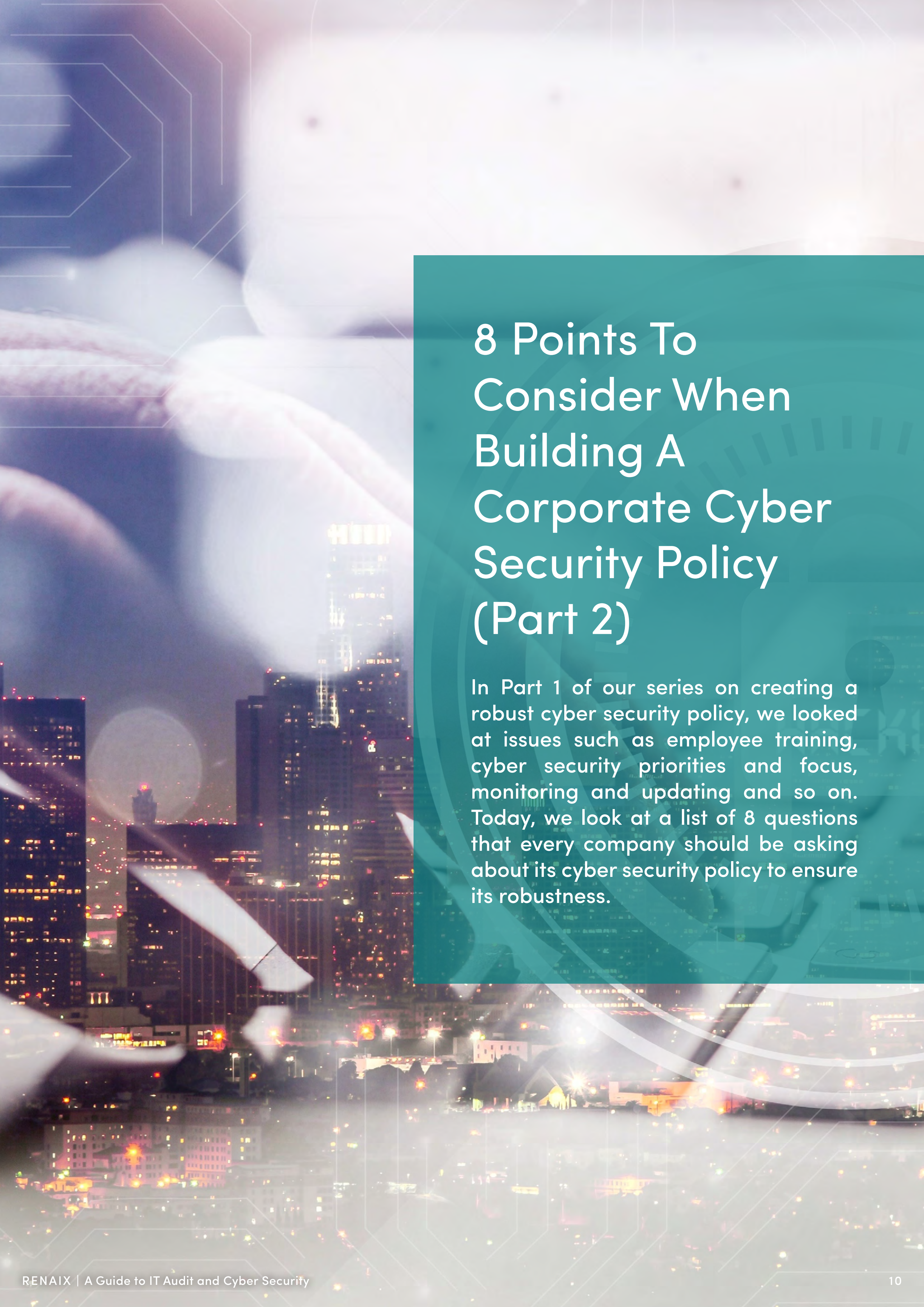
Having the strongest cyber security policies would mean little unless the weakest links are addressed. The weakest links are generally channel partners such as vendors who have access to a company's systems or information. Companies that provide access to sensitive information to their vendors should ensure that the vendors are not the weak links in their cyber security plans. Reviews of their policies or even surprise external audits might be mandated.

Employee Training

Internally, the weakest link when it comes to cyber security are the employees themselves. It's not complex hacking tools that are the biggest threats, it's employees being careless – setting up weak passwords, falling prey to social engineering scams, clicking or downloading something they shouldn't and so on. Any cyber security policy should take this into account and provide the relevant training to employees and sensitise them about these issues. It's not just sufficient to disseminate this information, it might make sense to have periodic quizzes even.

Monitoring and updating

The most menacing aspect of these cyber security threats is the speed with which they evolve. Stealing and selling data is one thing, but now we are seeing other things like holding data / emails hostage or even spreading false information with the intent of causing reputational damage. These things were not usually protected against before, but what use are policies if they only protect you from what was damaging last year?



8 Points To Consider When Building A Corporate Cyber Security Policy (Part 2)

In Part 1 of our series on creating a robust cyber security policy, we looked at issues such as employee training, cyber security priorities and focus, monitoring and updating and so on. Today, we look at a list of 8 questions that every company should be asking about its cyber security policy to ensure its robustness.

Is the cyber security policy aligned with the business strategy?

A lot of companies treat cyber security as solely within the IT Department's remit. This can result in situations where the cyber security will lag behind plans being made and executed by the business divisions leading to security policies always being out of sync and playing catch up rather than being integral to planning.

What's the level of importance that board members or senior executives place on cyber security?

Is it something that is discussed in Board meetings? Is it something that forms part of the Key Performance Indicators of the Business Units? Because it should be. The KPIs should not only track revenue but risks as well and this includes things like regulatory lapses or digital security breaches and so on.

What does the future digital footprint of the company look like?

Businesses and individuals are increasingly relying more on third-party vendors, sometimes without even realising it. Every time we use a web-based service like an online accounting tool or even Google Docs, we are sending our information to a third party. There is nothing wrong with this at all, but such external dependencies should form a part of the overall cyber security policy.

Does functionality trump security?

Are we willing to compromise on security if it is creating a functional bottleneck?

Are the policies being applied universally?

More often than not security breaches are not a result of an inadequate policy, but rather that the policy was not actually implemented fully. For example, a policy might call for user access to certain applications be restricted to just business heads, but then often they will delegate their authority or even share login credentials with staff.

How stringent are our third-party controls?

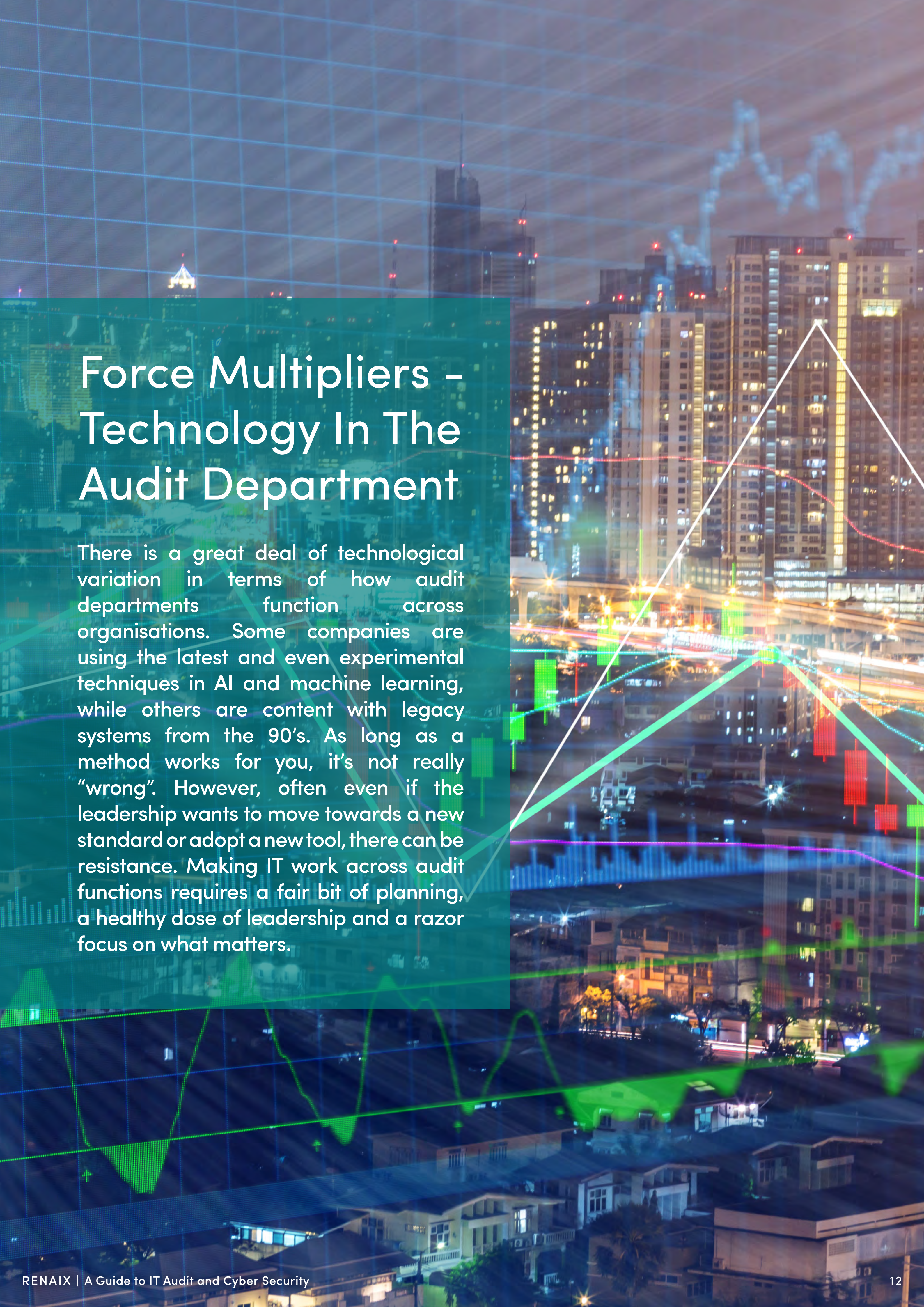
It is not uncommon for third party vendors to have access to certain critical data required for them to function. A lot of data breaches affecting big companies happen not directly, but rather through their vendors. Malicious actors are fully aware that small third-party vendors are the weakest links and that is where they focus.

How strong is our monitoring and vigilance?

How long would it take us to tell if a breach has even occurred?

How effective is our response?

Essentially nothing is a hundred percent secure. Even military departments get hacked on occasion. Therefore all companies should have a response plan prepared in advance rather than scrambling for one if and when a breach does happen. This response plan should include things like a backup contingency to fall back on, a plan to communicate it to relevant stakeholders, including clients, and a way to ensure that enough evidence gets recorded about the breach.



Force Multipliers - Technology In The Audit Department

There is a great deal of technological variation in terms of how audit departments function across organisations. Some companies are using the latest and even experimental techniques in AI and machine learning, while others are content with legacy systems from the 90's. As long as a method works for you, it's not really "wrong". However, often even if the leadership wants to move towards a new standard or adopt a new tool, there can be resistance. Making IT work across audit functions requires a fair bit of planning, a healthy dose of leadership and a razor focus on what matters.

Laying the groundwork

The change must start at the top. The leadership must be convinced that the new software tools, processes or other changes are actually going to provide the needed benefits. Once that has been achieved, it can trickle down throughout the workforce. These changes can be a significant expense and a very large percentage of companies often end up not using the new tools at all or abandoning them too quickly because they were never really sold on them in the first place.

Technology just for technology's sake never works. This first step is what will decide if the investment pays and off and the majority of decisions that go wrong, do so at this point itself.

Forcing it

This might prove to be an unpopular opinion, but sometimes the leadership will have to force through change and overcome whatever resistance they encounter. Making the use of technology mandatory might seem archaic but it can erode resistance and as people become more proficient with the new tools, it will invariably lead to improved efficiencies across the board. If that does not happen, then clearly some wrong decisions were made and which is why this article started with the "laying the groundwork" part. The foundations have to be right for it all to work.

Training

The best tank or fighter plane in a nation's arsenal is useless without the right training to operate it. Some companies make it a point to spend a certain fixed percentage of their total budget for a new tool/ process on training! What this means is that rather than overspending on something that won't be used properly, it might be better to split the cost across acquisition and training and use what was acquired at 100% efficiency.

Monitoring and Measuring

Improvement has to be a continuous, iterative process. The first step here is to set up measurable goals. This can be tricky in certain audit departments but results in Quality Assessment Reports can be one criterion for judging performance. Timelines, costs or workhours spent could be another criterion.

The best way to do this is to set these Key Performance Indicators at the time of setting up the new IT-driven process itself. Ask yourself why exactly is this new tool being acquired or developed? Is it to reduce costs? Then measure and monitor the costs. If it is to reduce errors or improve quality, then that has to be a part of what is measured and monitored.

Future Proofing IT Audits

Moore's law, which essentially talks about the doubling of transistors in a circuit every two years, is colloquially applied to almost all things tech. Irrespective of whether it still holds or not, we can all agree that the pace of technological advancement continues to be dizzyingly high.

What this means is that rather than learning about a tool or process and then happily applying it throughout one's career, we must keep learning new tools and technologies.

What makes things even more dynamic is that the marketplace is now global. So rather than competing with the business next door, you are competing with companies with vastly differing cultures, cost structures and regulatory burden (or lack thereof). Therefore, using force multiplication technologies has become extremely important for businesses. This is the topic of this post which covers how these force multiplies can be used in the field of IT audit now and in the future.

Constant Change

The first thing that must be embraced is that the only constant is change. Even if companies are willing to spend big on the latest tools, there will be new versions of tools coming out next year. How do you keep up?

Software-as-a-Service

One solution might be to use Software-as-a-Service. Rather than outright purchases, you are essentially subscribing to a service and whatever upgrades are made to that software, are delivered to you immediately via an update. The best part is that if you are not happy with the tool, you can switch over next month.

Cloud Service

Another technology which really compliments SaaS well is cloud service as this can be used for hardware as well. Afraid of servers getting outdated? Are your hardware requirements seasonal? Don't have the manpower to keep maintaining hardware locally and keeping up with the latest cyber threats? A cloud solution can alleviate most of that. Again, if you are not happy, switching is a lot easier.

Constant Training

With constant change must come constant training. It might be a good idea to dedicate a certain portion of employee time on just training. For example, 5 or 10 days a year or more based on the specifics. Complicated functions might even require 30 days or more! Some companies think of this as wasted time, but the investment is going to be peanuts compared to the potential financial and reputational loss in the event of a cyber breach or something similar.

Keeping up with the Buzzwords

Certain phrases are used so often that they begin to sound like buzzwords. AI, machine learning, cognitive intelligence, big data, advanced analytics and so on. However, there is a reason that these became buzzwords. Some of them might not be quite ready or cost-effective for small or medium businesses, but things like data analytics have repeatedly led to demonstrable improvements in efficiency especially in the audit functions where the data is voluminous.

Eventually, whichever tools are picked for use by an organisation they must meet its requirements and overall goals. Rather than going after buzzwords, it makes more sense to focus on what's important. It would be sub-optimal to start preparing for the future without first being 100% confident of what exactly you want to achieve in terms of IT security, audit controls and so on.

Thank you

if you enjoyed this guide, then look out for the next one...

RENAIX Ltd.
5A Underwood Street London N1 7LY
United Kingdom
+44 (0)20 7553 6320
info@renaix.com
www.renaix.com