Grant Thornton

An instinct for growth™

Cyber security

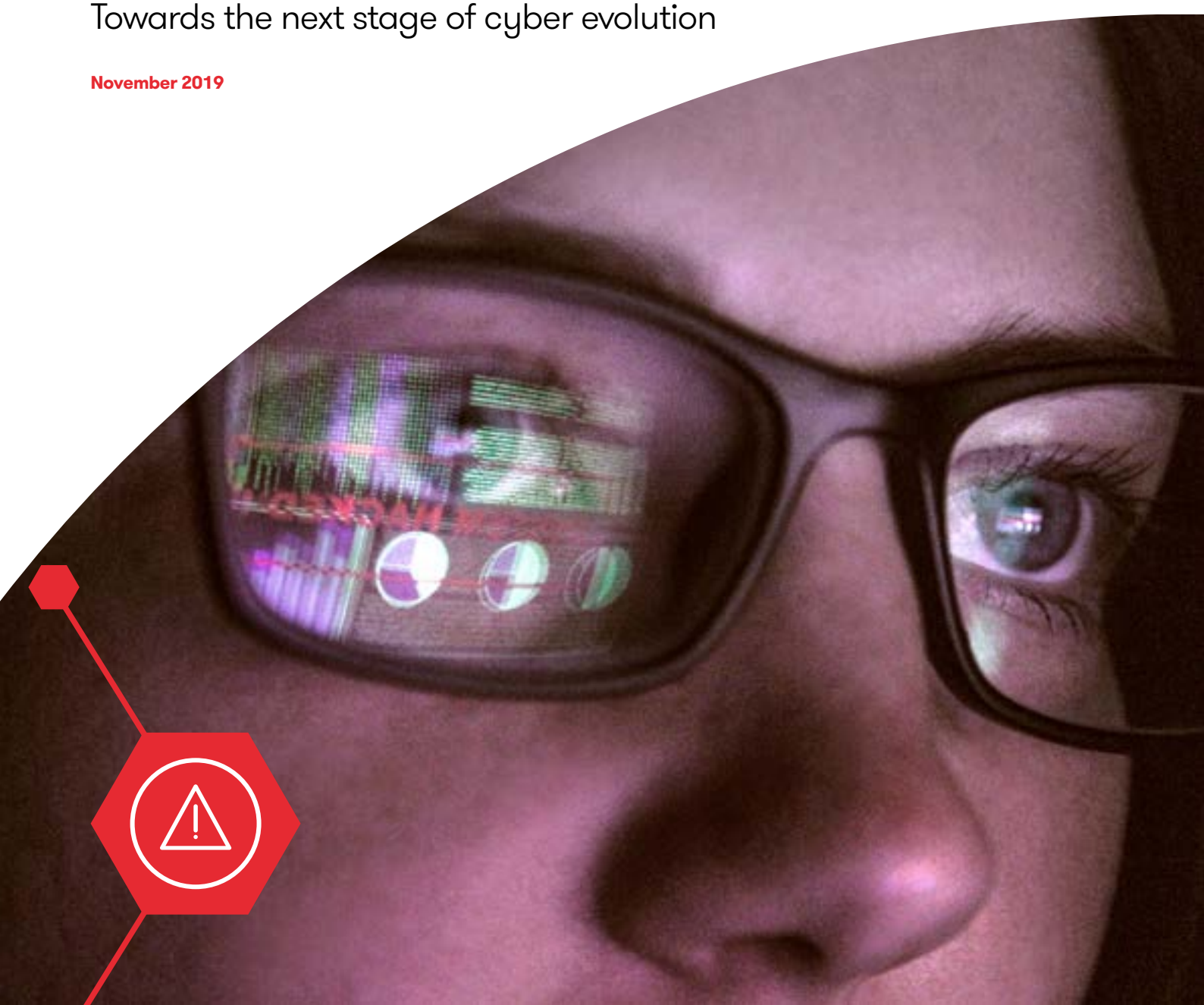
Advisory

Risk

How to better manage digital risk

Towards the next stage of cyber evolution

November 2019



Introduction

Businesses of all shapes and sizes are trying to carve out competitive advantage by leveraging digital information. But owing to the increased use of personal data, it also creates vulnerabilities and inter-dependencies between two previously discrete threats – data privacy and cyber security.

Our IBR research found businesses are laser focusing on mitigating data privacy risk. That's no surprise, given the proliferation of data privacy regulation. But cyber threats continue to soar. So what's the solution? Our advice is to build a wider 'digital risk' function which integrates data privacy and cyber security. But where should you start?

The articles below explore the findings and make recommendations for bolstering your digital risk management.

Strategically aligned, competitively distinct

It's time to merge cyber security and data privacy into one digital risk function.

Businesses of all shapes and sizes are trying to carve out a competitive advantage by leveraging digital information. The most cutting-edge companies harness customer preference data for a range of reasons, including to create personalised services and targeted marketing campaigns; to scrutinise employee performance data to drive productivity; and to analyse supply chain information to drive efficiencies. And that's just the tip of the iceberg, with digitised data embedded across business practices.

Digital information offers businesses huge potential, but owing to the increased use of personal data, it also creates vulnerabilities and interdependencies between two previously discrete threats – data privacy and security. For example, data breaches can result from a cyber attack, but have data privacy implications.

GDPR and other international data privacy regulations have started to bite, meaning businesses are starting to feel the commercial cost of data privacy violations. So it is perhaps no surprise that we see data privacy rising up the business agenda. Grant Thornton's research of over 4,500 international business leaders found that 2 in 3 agreed that due to new regulation there has been a greater focus on privacy issues than there has on cyber security in recent years in their business.

However, it's important to not lose focus on the real and growing cyber security risk - the number of cyber attacks causing losses in excess of $1m has increased by 63% during the past three years.

Mike Harris, partner, cyber security services at Grant Thornton Ireland emphasises that data privacy and cyber security have never been more interlinked.

"In today's data-driven world, data privacy and cyber security simply cannot be considered in isolation," he says. "They should be viewed instead as part of a wider digital risk function."

But what is 'digital risk'?

Digital risk is a business-driven model that proactively considers the business risks associated with digitised data across business processes, including cyber security and data privacy, along with other considerations such as regulation, automation and ethics.

Think about how you secure your own home. Do you one day focus on locking all of the doors, but happily leave the windows and open? And on another day, would you ignore setting the alarm, because you are too busy focusing on securing access from the garden? Of course not – all of these risks need to be considered together, or your protection measures will quickly fail.

It's a similar story when assessing a company's digital risk profile – focusing on each of the threats separately is no longer effective, and instead they must be proactively integrated and managed together. It's only when a business takes a holistic approach like this that real progress can be made.

Indeed this integrated best practice is embedded in the regulation. The General Data Protection Act (GDPR) states that, in order to be compliant, companies should implement 'data protection by design and default' measures. The Information Commissioner's Office explains that this means companies must "integrate or 'bake in' data protection into… business practices, from the design stage, right through the lifecycle". It would be very difficult indeed to 'bake in' such privacy measures across the business without a single, integrated function.

So it is critical for businesses to effectively and efficiently get to grips with digital risk. Yet they are struggling, because data privacy and cyber security are often managed by different teams. Typically the Chief Privacy Officer (CPO) takes responsibility for the data privacy; while the Chief Information Security Officer (CISO) for cybersecurity.

It would be far better for both to be managed by the same team or an integrated team with new governance model which provides a direct reporting structure to the CEO/CRO (Chief Risk officer) with oversight from a board. After all, a lot of work that ensures compliance with data privacy can be used to bolster cyber security, and vice versa. In addition to helping businesses manage digital risks, this approach adds value by enabling them to bring forward digital transformation initiatives.

[3] Global cyber-incidents soar by 63% in the last three years, Linklaters, January 2019

Optimising data classification

A single digital risk team will also ensure the data classification that companies are undertaking across the business for various purposes is aligned and co-ordinated.

Data classification means understanding what data is held by the business, the processes it connects to, and who manages it. It is a crucial part of compliance with data privacy regulations such as GDPR, but can also be used to enhance cyber security.

By undertaking a structured programme to assess and understand their data assets - using a categorisation or classification process - business can identify their key data and build effective security around them.

Harris adds: "We see that the Pareto principle applies to data risk in many businesses, with 20% of a business's data carrying 80% of the risk. It is almost impossible to make all systems hack-proof, so why not focus on the data for which security is absolutely essential to your business and to your customer?"

Hans Bootsma, partner, cyber risk services at Grant Thornton Netherlands, agrees that an integrated approach to privacy and cyber security extends to the classification process.

"Most companies never classified data before GDPR," he said. "But they started to because they had to categorise personally identifiable information and other types of data in order to comply. If you run a programme like this, then it's easy to extend it and combine it with other types of data to identify your data crown jewels and then link this with your cyber programme."

Unless data privacy and cyber security are aligned, the classification process will happen in isolated silos and the benefits will not be shared.

An integrated response to breaches

The interconnection between data privacy and cyber security is never more painfully obvious than immediately following a data breach. Businesses need to know how the breach occurred and which cyber defences (if any) failed. But, crucially, they also need to understand which data were compromised and whether it was personal or sensitive. If so, they will need to disclose it.

Most businesses are not fully equipped to do this. Only 28% of businesses surveyed by Grant Thornton are 'highly satisfied' with their ability to protect against the risk of a serious breach and just 26% with their ability to respond consistently to a major breach across the entire business, no matter when or where it takes place.

Integrate privacy and security into one function, and businesses will be able to respond more effectively to data breaches due to their combined resources and holistic understanding of the threat.

"Privacy and cyber security are complex because they are crashing together in the real world," says Harris. "A data breach could start off as something very technical in an outsourced cloud provider. But in responding to the incident you need to consider whether personal data are involved and what regulatory disclosures need to be made.

"All of a sudden, the two have become interconnected. Rather than two separate cyber and privacy functions responding to a breach, it makes sense to have one integrated function with the specialised skills to manage the process, so that nothing falls through the cracks."

Managing supply chain and third-party digital risk

The increased interconnectedness of cyber security and privacy has implications for how third-party risk is managed. For example, data privacy regulation such as GDPR requires businesses to get robust guarantees from suppliers that handle data on their behalf.

"It would make a lot of sense for organisations to merge cyber security aspects of third-party risk management with privacy controls," says Harris. "It's just a matter of asking about both at the same time. It's relatively straightforward, but it's not happening widely at the moment. Cyber security teams and privacy teams are doing this separately."

Of course, this 'one-stop' third-party risk management will remove duplication of effort and create efficiencies. More importantly, however, it will produce a more joined-up understanding of digital risk.

Benefits of an integrated digital risk approach

Taking an integrated business approach to managing digital risk delivers a number of key benefits to organisations.

Firstly, it can help to bring forward digital transformation initiatives because the data classification and compliance that companies are undertaking across the business for various purposes is aligned and co-ordinated.

Secondly, a digital risk function that conducts comprehensive assessments of third-party and supply chain digital risk is better positioned to ensure that risk is considered across the organisation. One way to do this is by pre-approving vendors from a risk perspective.

"Businesses can digitally transform quicker if they do the supplier approval process up front," says James Arthur, partner, head of cyber consulting, Grant Thornton UK. "It's a lot easier to do this if you have a single digital risk function that proactively assesses cyber security and privacy risk together."

Thirdly, businesses continue to use new technologies to seek out commercial advantage, meaning their approach to data privacy and cyber security also needs to continually evolve, to address new threats and vulnerabilities. An integrated digital risk function is better placed to scrutinise some of these new technologies, such as blockchain.

"It's vital that risk teams are involved right from the outset, because with any technology database there's always the risk of attacks by third parties that want to steal the information" says Michel Besner, general manager of Catallaxy, a blockchain subsidiary of Raymond Chabot Grant Thornton. "To combat this, risk teams can ensure that there are proper governance structures around how the blockchain is implemented, managed and supported. Get this right, and you'll avoid security issues further down the line."

Board oversight is key, combined management essential

The case for an integrated digital risk function is clear. But who should oversee and manage it?

At the moment, there is confusion about where responsibility ultimately lies, and this is hampering digital risk management. Tellingly, surveyed businesses say that a lack of understanding about which risks individuals and teams are responsible for is their second-greatest weak point in managing digital risk.

The first important thing to consider is who manages digital risk from a day-to-day point of view. Most companies put the chief risk officer or chief technology officer in charge of this. But, as explained in our Digital risk: Technology is no silver bullet article, effective digital risk management relies on a lot more than technology. Chief risk officers report on more holistic risk to business – strategic, financial and operational. So what's the answer?

Enter the chief digital risk officer function. "Organisations are starting to create digital risk functions headed by a chief digital risk officer," confirms Arthur. "This is where responsibility for managing digital risk should lie. But at the moment they are still organisationally distinct at most companies."

Once the day-to-day digital risk management is in place, its essential to consider who provides oversight. As with financial risk, the gravity of digital risk means that the board must take an active role. While the board needs to oversee it, they may not always have the technical expertise to understand the nature of the threat. Therefore ideally, a specific digital risk committee should be established within the board to oversee this risk, with representation from experts.

"Digital risk oversight should be at board level," confirms Christos Makedonas, technology risk leader at Grant Thornton Cyprus. "There should also be a committee that discusses digital risk.

"Digital risk is multifaceted, so many people need to feed into this process. At the moment, this only happens in large, heavily regulated companies – especially those in financial services."

Three steps to integrated digital risk management

1 Work out who is responsible for managing cyber security and data privacy risk, map out their activities and daily workflows, and see if there is any overlap. Strip out duplicated processes.

2 Ensure that digital risk processes are managed on an end-to-end basis. For example, third-party assurance should assess both cyber security and data privacy. Both factors should also be evaluated when classifying data.

3 Create an integrated digital risk management team or function that has the skills to manage both cyber security and data privacy threats. Head it up with a chief digital risk officer capable of championing digital risk and ensuring it's factored into strategic and operational decisions across the business. Make sure that the board actively oversees digital risk.

Technology is no silver bullet

Businesses rely too heavily on technology to fight cyber threats. Risk management, processes and skills are crucial weapons.

Businesses have ploughed billions of dollars into technology that promises to keep cyber threats at bay. Gartner[1] claims that end-user spending for the information security market is estimated to grow at a CAGR of 8.5% between 2017 and 2022, reaching $170bn.

While technology undoubtedly plays a major role in combating digital threats, other areas have been neglected. Tellingly, mid-market business leaders surveyed in Grant Thornton's International Business Report (IBR) say that over-reliance on software is their weakest point in managing cyber and privacy-related threats.

It's encouraging that business leaders acknowledge this. But now they must act, by improving their employees' awareness and specialist skills in cyber security.

This doesn't necessarily mean spending more money. In many cases, companies will be able to taper technology spending as they strengthen and invest in their business acumen, processes and in-house skills.

Customer trust is built on more than technology

"It is essential that businesses understand that investing in technology alone is not the only answer to reducing digital risk, and it will not protect them from losing customer trust should the worst happen" says Mike Harris, partner, cyber security services, Grant Thornton Ireland. "A key starting point for companies is understanding the type of business they're in, and the value they deliver to the customer". Once this is understood, companies will have a clearer idea of the potential impact a breach would have on that relationship, and can better work out how to mitigate this, through a range of measures. Internal governance, processes and people are the other crucial ingredients here.

Take a casino chain as an example. Many casino customers are high-net-worth individuals, who take the security of their financial data – such as transaction history and payment information – extremely seriously. The casino can have the best technology systems in place to protect this data, but it is not enough in isolation. The company must have robust governance procedures, customer relationship managers and trust policies in place to complement the technology and to protect the company's reputation in the event of a breach. In this example, the value the casino provides to its customer revolves around customer service, trust and entertainment – with technology acting simply as an enabler to make this happen. Therefore, the company's approach to digital risk must mirror this – with robust trust procedures around in place, complemented by top-class technologies.

[1] Gartner Forecast for Information Security Worldwide, 2016-2022

Boosting awareness of human risk management

Understanding that there is more to managing digital risk than relying on technology is just the first step. Companies must then take a number of non-tech measures to protect themselves.

New ways to raise awareness

Companies might be investing in sophisticated cyber security technology, but that won't necessarily prevent the human error that's behind many cyber breaches. After all, it's the human workforce that responds to phishing emails and installs unauthorised software.

Managers can address this by increasing awareness of cyber security issues across the business. But how to do this effectively? Businesses have been running cyber security webinars and mandatory training programmes for many years, yet human error continues to open them up to cyber attack. A new form of education is necessary.

Christos Makedonas, technology risk leader at Grant Thornton Cyprus, says that shorter training formats would help. "No one has time to watch hour-long training videos," he says. "They should be shortened to a maximum of two minutes. You also need visual reminders – such as banners around the office and messages on screens – to remind people of best practice.

"Businesses should then simulate phishing attempts, and the employees that respond to them can then be given further training. We've found these sorts of training programmes to be much more successful than conventional webinars."

Identify vulnerabilities first, invest later

Businesses need to understand where they are vulnerable to cyber attacks and data-protection breaches before investing in preventive software. This requires specialised skills that most cyber security functions don't have.

"Businesses need cyber security and privacy-related skillsets to help map out their data and understand their regulatory requirements – particularly in a cloud environment," says Harris. "They also need cyber technology skills around the technologies they are using.

"For example, if you are using cloud services provided by Amazon or Azure, you need to have the security skills in house to work out what they will and will not do regarding cyber security. That skills component is often overlooked."

Advanced analytical tech needs advanced analytical minds

Many businesses have invested heavily in advanced analytical cyber security technologies that help identify new threats and vulnerabilities. But these are only as good as the workforce that can interpret the results and implement corresponding changes.

"Lots of people look to technology as a silver bullet, but it isn't," says James Arthur, partner, head of cyber consulting, Grant Thornton UK. "Many companies spend a lot of money on AI-driven, behavioural analytics cyber security software, which can be really useful in some circumstances. However, you normally need to spend an awful lot of human time training it to ensure it delivers useful insights. Then, you need a human at the end of that chain who can look at the output and make/approve changes."

Insure against the inevitable

"There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." These are the words of former FBI director Robert Mueller back in 2012.

His message is clear – and just as relevant today as it was seven years ago: a breach is inevitable. It makes a strong case for investing in insurance as another way to manage digital risk.

"Any reasonable cyber security programme has to have an element of detection, response and insurance, because cyber events will happen," says Harris. "We see increased adoption of insurance that covers both cyber attacks and data privacy regulatory breaches. But while it's imperative and its use is increasing, the majority of businesses still don't have this type of insurance or aren't protecting the right data assets."

Understand your most valuable data assets and protect accordingly

Businesses should undertake a structured programme to assess and understand their data assets, using a categorisation and classification process. Then, they can identify their 'crown jewels' and invest in appropriate insurance cover.

But how do you do this? One way to identify your most critical data is to think like a hacker and then consider the maximum damage they could cause. "The current data security environment is consistently evolving with new threats and vulnerabilities," says Harris. "Leaders have to be willing to step into the shoes of cyber criminals, understand the threats these groups pose and come up with proactive strategies to protect their business' interests."

Which email threads could a former employee leak to embarrass their former managers? What intellectual property and trade secrets would be of interest to a foreign power? And how might a cyber criminal use your data to try to extort money from your business? These are just some of the questions you need to ask before purchasing insurance as part of your digital risk management plan.

Five recommendations for creating a balanced approach to digital risk management

1 Companies must understand that the increasing amount of data that customers share with brands means that trust is more important than ever. It's essential that businesses understand the necessity of trust management, and that digital risk policies and procedures go a long way to ensuring this.

2 Traditional approaches to cyber training are not working. Businesses should develop shorter, more frequently distributed training videos and simulate phishing attempts to better educate their workforces.

3 Businesses need to identify and map out their digital vulnerabilities. They need to recruit staff with specialised cyber skills that complement cyber security technical skills. This will ensure that their investment in preventive software is focused on the right areas.

4 All businesses will suffer a cyber attack – no matter how much they invest in preventive software. Investing in insurance can bolster your risk management but it is crucial to insure your most valuable data assets and

5 Once insurance is secured, businesses must be vigilant about adhering to the terms and conditions. If they fail to install updates, it could nullify the insurance.

Contacts

We help our clients prepare themselves for cyber threats, ensure ongoing protection, reactive effectively and drive change to improve their digital risk management capability.

To explore how your business could improve information management and minimise risk, please contact one of our member firm specialists.

UAE

George Stoyanov
E george.stoyanov@ae.gt.com

Samer Hijazi
E samer.hijazi@ae.gt.com

Mohamed Elewa
E mohamed.elewa@ae.gt.com

Avik Chandra
E avik.chandra@ae.gt.com

IBR 2018 methodology

The Grant Thornton International Business Report (IBR) is the world's leading mid-market business survey. Launched in 1992 in nine European countries, the report now surveys more than 10,000 senior executives in 35 economies on an annual basis, providing insight into the economic and commercial issues affecting both listed and privately-held businesses. Fieldwork is undertaken on a biannual basis, through both online and telephone interviews.

IBR is a survey of mid-market listed and privately held businesses. The definition of the mid-market varies by country; in the EU, we interview businesses with 50-499 employees; in the United States, we interview those with annual revenues of USD20m to USD2bn; in China, those with 100-1000 employees. Respondents are chief executive officers, managing directors, chairpersons or other senior decision-makers.

For more information:
grantthornton.global/About-IBR/
E gtimarketing@gti.gt.com

About Grant Thornton

We're a network of independent assurance, tax and advisory firms, made up of 53,000 people in over 135 countries. And we're here to help dynamic organisations unlock their potential for growth. For more than 100 years, we have helped dynamic organisations realise their strategic ambitions. Whether you're looking to finance growth, manage risk and regulation, optimise your operations or realise stakeholder value, we can help you. We've got scale, combined with local market understanding. That means we're everywhere you are, as well as where you want to be.

Grant Thornton

An instinct for growth™

grantthornton.global

EPI.311