Grant Thornton

An instinct for growth™

Cyber security

Advisory

Risk

Locking down the value of data

A shift in risk-management priorities

2017

Contents:

Executive summary

Getting to the heart of cyber risk

Today's senior leaders face a range of complex, interconnected and fast-evolving risks. Few of these are as critical and so poorly understood as the risk of cyber-attack.

One of the main challenges is the non-physical nature of the threat. Data is a long way from the traditional property that can be neatly defined and covered by standard business insurance. All too often, the potential for a cyber-attack is regarded as an IT problem rather than an enterprise-wide issue. Yet a serious breach can cause catastrophic harm: it undermines customer trust, provokes regulatory scrutiny, disrupts operations and causes long-term financial damage.

We carried out research with one question in mind: how do today's leaders ensure that their businesses can anticipate and overcome cyber risk?

We wanted to go beyond the jargon, technical language and media scare stories to outline a practical approach for today's leaders that would make a cyber-attack a more manageable threat. In particular, we wanted to think about the risk to data, because that is what businesses are ultimately trying to protect from hackers.

"Our view is that effective management of cyber risk is only possible if businesses have a clear picture of the data they have," says Paul Jacobs, global leader of cybersecurity at Grant Thornton. "That could be their email server data, financial information, customer records, proprietary processes or trade secrets. Only when they fully understand the importance of this data and where it is stored – which is known in some circles as categorisation or classification – can they implement hacker-proof defences where they are needed most."

To understand the level of business maturity in this area, we surveyed 2,900 senior executives through Grant Thornton's International Business Report (IBR).[1] We also interviewed 12 individuals – from the Grant Thornton network as well as from academia and business – who have expertise in cybersecurity and information management.

"Most organisations think a breach is not going to happen to them. Perhaps 20% feel they'll be attacked soon, and thus they've invested in sophisticated cybersecurity systems to prepare for such. About 30% are probably quite well-prepared. The rest are in the middle or believe such cyber-attacks won't be targeted against them."

John Kan, chief information officer, A*STAR

1. Grant Thornton research undertaken in Q4 2016. Full methodology at the end of this report

Key findings

What businesses know, say and do about their critical data

Too many businesses are in the dark about the data they hold

Every business, every day, generates an incredible amount of data. The easiest and cheapest way to store all this information is to adopt the 'landfill' model of keeping everything and moving as much of it as possible to the cloud. But we find that many are doing this without even trying to keep track of what they have.

Our survey suggests that less than two in three businesses (65%) are taking steps to understand their data; they are largely in the dark about how much there is, what it does, and what harm it could cause if compromised. And if they don't know these basics, how can they be sure they are looking after it properly?

There is a data-shaped hole in most risk management

More than one in three (36%) organisations do not assign a risk profile to their data. Considering what they stand to lose if their data is compromised, this is surprising. One explanation may be that, although the C-suite accepts that cybersecurity is a risk, leaders are still not doing enough to directly 'sponsor' mitigation efforts.

Another explanation is that the risk function has largely focused in the past on a limited number of business risks that can be insured. As a result, legacy risk teams are less experienced in predicting, managing and pricing non-physical threats such as data breaches. This needs to change.

Many businesses are 'protecting everything, protecting nothing'

More than three-quarters of businesses (78%) are building a baseline of cyber protection without putting in place specific measures to lock down their most precious data. At worst, this means they are implementing expensive firewalls that protect data of little value, while their most critical information assets – those which are necessary for the business to carry out its core function – are more exposed than they should be.

30%

are probably quite well-prepared

50%

are in the middle or believe such cyber-attacks won't be targeted against them

20%

feel they'll be attacked soon, and have invested in sophisticated cybersecurity systems to prepare for such

Understanding data means balancing lateral and vertical thinking

For most organisations, it would be practically impossible to assess and rank every spreadsheet, archived email or data file that is generated every day. It's also a process that cannot be completely automated: understanding the risk and value of data requires human judgement.

Getting it right also takes imagination: being able to think like a cynical and opportunistic hacker and identifying data that would disrupt the business if compromised or compounded. Yet qualitative reasoning should also be counterweighted, as much as possible, by quantitative analysis. What would be the financial impact of a major breach? Would the impact always be the same? And what is the statistical likelihood of it happening?

People are the weakest link

Getting to grips with data is time-consuming and, to be successful, needs to become part of business as usual. This means creating enterprise-wide leaders of the activity as well as individual owners of data assets.

Yet many employees, given responsibility for data on top of their day-to-day tasks, try to sidestep the extra work. At worst, we see passive avoidance – where employees mark data as being lower risk than it is purely in order to get out of the 'hassle' of protecting it from hackers.

To manage cyber risk effectively, businesses need to anticipate this reaction from employees and take steps to prevent it from happening.

There are three principles to managing data risk more effectively

First, data security should be treated as an enterprise-wide, consistently applied risk that is led by the C-suite and then implemented by employees at the operational level. Second, data understanding needs to be built into projects by design, with a multidisciplinary team seeking agreement on the biggest data-related threats to the business. Finally, all engagement – whether communications from the top or training – needs to take place on a human, non-technical level.

A serious breach can cause catastrophic harm, it:

- undermines customer trust
- provokes regulatory scrutiny
- disrupts operations
- causes long-term financial damage.

Are you defending the wrong data?

A business today is only as good as its data. The better your information – whether customer records or employee data, process documentation or daily outgoings – the better your ability to plan ahead, make decisions and manage your operations.

Anything that is important is a source of risk. If sensitive data is compromised, you face reputation damage, financial loss, heavy fines (see box, 'EU General Data Protection Regulation'), business disruption and customer churn. This is why information security risk has shot up the boardroom agenda, regularly appearing among the top risks identified by global insurers[2] and the World Economic Forum's Global Risks Report.[3]

Yet our global survey of 2,900 businesses suggests that many do not have a clear picture of the data they hold or its overall importance. Less than two in three (65%) are taking steps to fully understand what data they have; only about half (56%) assign a risk profile to their information.

Misplaced defences

Our findings beg a simple question: if organisations don't know what data they hold, or how important it is, are they wasting time and money safeguarding low-value information while their most critical assets are exposed?

The answer is almost certainly yes. About four in five respondents to our survey (78%) admit that they tend to spread their protection measures evenly across all their data. Only the remainder stress that they put in place special safeguards to protect their most vital information.

A vice president (VP) of technology at a global bank, interviewed for this report, warns of the danger of not allocating specific controls to higher-risk data. "I see critical data being put on SharePoint," he says, referring to the web-based file-storage platform. "Many provide access to critical data on sharing platforms by default."

The 80/20 of data

We estimate that the Pareto principle applies to information risk, with 20% of a business's data carrying 80% of the risk. For Tom Faulkner, head of IT production at CMC Markets, the ratio is even more extreme. "There's a very thin top tier of data, maybe 5% of the overall, which has to be precise and protected to the highest standards as it cannot go missing," he says. "Then we have a significant quantity that needs to be accurate and adequately protected."

There is a well-known saying: 'To protect everything is to protect nothing.' It's almost impossible to make all systems hack-proof, so why not focus on the small amount of data for which security is absolutely essential?

2. http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf / https://www2.chubb.com/TR-TR/_Assets/documents/20150707_EMERGING_RISK_BAROMETER_FINAL_PUBLISHED.pdf
3. http://www3.weforum.org/docs/GRR17_Report_web.pdf

"If you have to pay $X to buy state-of-the-art firewalls, IPS, IDS devices, but the total economic impact of a breach is less than $X, then some organisations may prefer to take the risk and not invest in such expensive security devices, or perhaps install a less sophisticated cybersecurity framework instead," says John Kan, chief information officer at A*STAR in Singapore.

With this in mind, it is our firm belief that businesses should undertake a structured programme to assess and understand their data assets, using a categorisation/classification process. Then, they can identify their 'crown jewels' and build effective security around them.

"Step number one is acknowledging that your information assets are not equivalent, step number two is conceding that a compromise is likely to occur. It follows that you would focus on protecting the higher-value assets."

Johnny Lee, Grant Thornton US

EU General Data Protection Regulation: The global implications

From 2018, the cost of a data breach will become more direct and will have greater financial consequences. In May 2018, the EU's General Data Protection Regulation (GDPR) will fine businesses up to 5% of global turnover for losing customer data. Once GDPR is in place, we can expect other jurisdictions worldwide to enforce similar regulations.

To put this change into context, the recent cyber-attack against Tesco Bank, UK, which led to the breach of 9,000 customers' accounts, led to the bank reimbursing a total of £2.5m. If the breach had occurred after GDPR comes into force, the bank could have been fined £2bn.

Crown jewels: The what and the why

It is extremely difficult, in a digital-enabled world, to keep track of all the data your organisation creates and gathers every day.

IBM calculates that nine-tenths of all the data in the world has appeared in the past two years alone[5]. Others believe that we will live on a planet that contains 40 zettabytes of data by 2020[6] – which we estimate would be enough reading material to fill 50 billion human lifetimes.

So how do you find your crown jewels and your most sensitive data among those bytes? What constitutes high-, low- and medium-risk data? And against which threats – from state-sponsored agents at one extreme to disaffected teenagers on the other, with organised criminals, disgruntled employees and 'hacktivists' in between – should you prioritise defence?

Confidentiality, integrity, availability

First of all, it is unrealistic to try to rank every spreadsheet, archived email or data file your organisation holds. And you cannot fully automate the process: there are tools that support data management, but human judgement is always required at some point. Ultimately, you need to ensure that your senior managers and risk personnel actively consider the different kinds of data they own – this way, they can isolate the assets that need to be looked at more closely.

"We've created questionnaires so our personnel can make a decision themselves," says the VP of technology at a global bank. "It's subjective. At the end of the day, it's a person making a decision."

In the next section, we recommend practical ways to ensure that your employees engage in this activity. But what should they be flagging?

Many organisations adopt a dynamic model that evaluates data according to confidentiality, integrity and availability (CIA), and can be tailored to reflect changes in the data's importance or relevance over time.

"Board strategy papers are confidential until the time they go public and need to be protected," says Manu Sharma of Grant Thornton UK, explaining the CIA approach. "For integrity, the information may be available to everyone but it has to be accurate – the share price from the New York Stock Exchange is a good example. Availability is whether people who need the data can get it and use it, like marketing lists."

5. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
6. https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Thinking like a hacker

Another way to identify your most critical data-related risks is to think like a hacker and then consider the maximum damage they could cause.

"The current environment of information security is consistently evolving with new threats and vulnerabilities", says Vishal Chawla of Grant Thornton US. "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.

Companies in the supply chain and logistics industry could face a near-existential threat if hackers compounded or manipulated their data. Dr Ayman Omar, associate professor at the Kogod School of Business, has a background in supply chains and understands the risks. "If you're sending high value items, people could access the shipping distribution data and attack the physical shipment," he says. "We've seen people going after companies' suppliers – getting them off the grid and forcing the company to pay ransomware money to avoid delays."

A hospital in the US provides another example of how hackers could compromise the data that an organisation needs to carry out its core business activity. Cyber-criminals could, for example, change its patients' medical records and amend their blood types, before demanding a payment in return for changing the records back to how they were. If the hospital didn't comply, its patients could – within the half-hour – be given the wrong drugs. The outcome would be much worse than if the hospital had simply lost those same patients' credit card data.

Even seemingly trivial data files can be used to cause significant harm, as Ross Anderson, professor of security engineering at the University of Cambridge's Computer Laboratory, explains: "One place I advised took the view that, if their data got compromised, they'd just get a fine. I said, 'how would you feel if all your emails, with all the backstabbing and the rest of it, ended up on WikiLeaks or Pastebin?' The directors went white and cybersecurity went straight to the top of their risk register."

> "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."
>
> **Vishal Chawla,** Grant Thornton US

Reasons to be fearful: Threats to critical data by sector

Here we outline some of the threats by sector, with insight from Grant Thornton industry experts.

Healthcare

- Compounded patient records used for blackmail/ransom
- Corrupted facility information, such as hospital air-conditioning controls, used for ransom
- Stolen or compounded data relating to drug delivery and storage

"All healthcare organisations should be challenging the status quo on which IT functions deliver value and which are a commodity. It starts with understanding and prioritising your data from a clinical and business standpoint.

In healthcare, if a critical system is breached or fails then people can die. IT should have a strong focus on educating end-users about the continual need to manage security, which is not a single event – but rather a state of mind."

Anne McGeorge, Grant Thornton US

Financial services

- Stolen or compounded customer records used for fraud/ransom
- Seized market/trading data leading to operational paralysis
- Introduction of algorithms to disable/distort automated trading activity

"Global financial services is facing a perfect cyber storm. There is an increasing reliance on digital technology, while criminals are focused more and more on comprising systems as shown by the recent SWIFT incidents and rising concerns over payment systems. These issues coupled with the clear regulatory focus on cyber risk management mean many are struggling to respond effectively.

Financial services organisations should focus first on building a robust risk-based cybersecurity program. This will help achieve strategic goals while complying with regulatory requirements. Ultimately, you can speed innovation by focusing on cybersecurity up front."

Mike Harris, Grant Thornton Ireland

Energy and natural resources

- Corruption of GIS data that tracks the location of gas or electricity in the network
- Oil-well safety and mapping data compounded/ held to ransom

"The notion of a fully connected world where all systems and people are connected and every system can be accessed online is extremely dangerous. Think about dams; or nuclear power stations – hackers have proven that they can breach the highest levels of security. These critical infrastructure facilities, among others, are sitting ducks for teams of hackers, bent on wreaking havoc."

Michiel Jonker, Grant Thornton South Africa

Public sector

- Theft of data integral to the delivery of emergency services
- Corruption/ manipulation of economic and trade data by overseas agents
- Theft of state secrets

Consumer products

- Theft of manufacturing process information
- Corruption or theft of transport/supply-chain documentation
- Stolen intellectual property and R&D data

"The volume of sensitive data stored, managed, and processed by government entities is many orders of magnitude greater than some of the world's largest companies.

A single government agency may also need to secure numerous varieties of high-value information including personally identifiable information, healthcare records, patents and trade secrets, as well as banking information. Given all of this, and with limited resources to invest in tools and cyber expertise, agencies need to shift from a checklist-based compliance approach to a risk-prioritised, continuous monitoring model."

Scott King, Grant Thornton US

Real estate and construction

- Corruption/theft of building material specifications for ransom
- Corruption/theft of transportation/ supply-chain documentation
- Introduction of 'inherent vice' into building plans in order to cause future structural weakness

Travel, leisure and tourism

- Theft/corruption of tourist passport/visa data for fraud
- Stolen or compounded data essential for public transit systems
- Corrupted/compounded traffic-monitoring or control data
- Technology, media and telecommunications
- Compromised customer records
- Disruption of key communications networks
- Stolen intellectual property

"With technology at the epicentre of corporate and consumer lives, technology companies are ripe targets for cyber attack. They have the dual challenge of protecting their corporate assets while hardening their products and infrastructure which provide the backbone for e-commerce and social media.

The vast amount of value that data generates and carries needs to be protected at each step."

Steven Perkins, Grant Thornton US

Balancing qualitative and quantitative evaluation

Consistent, qualitative assessment of your data is essential, but you shouldn't neglect quantitative evaluation. This means estimating the financial impact of a breach as well as calculating its probability.

Kogod School of Business' Omar believes that many businesses put too much emphasis on subjective analysis. "Top management are asked to say on a scale of zero to five what they think of the company's risks," he says. "The reality is that it's no more accurate than simply doing nothing. You're not quantifying the chance of the risk happening, or the dollar impact. If you say the impact is 'three', what does three mean?"

He adds that undertaking a quantitative assessment of impact and probability involves analysing the incidence rate within the organisation as well as among others in the industry.

Checklist:

The potential 'crown jewels' of data

- ☐ Research and development data
- ☐ Regulated data sets: health data, financial transaction data
- ☐ Credit card data and other payment information
- ☐ Proprietary processes
- ☐ Email server data containing the email traffic of senior team
- ☐ Trade secrets
- ☐ Personally identifiable information
- ☐ Intellectual property
- ☐ Financial information

Barriers to success

A relatively high proportion of organisations do not understand their data or successfully manage the associated risks. Less than two in three (65%) are trying to fully understand the data they hold, and only half (56%) assign a risk profile to this critical business asset.

But getting to grips with data is not easy and cannot be taken lightly. As they try to understand their data, businesses must overcome several challenges.

1. Legacy risks and emerging threats: A disconnect

In many businesses, the risk function was established to track, measure and mitigate a defined list of insurable business risks. These legacy teams are often less experienced in managing fast-evolving, non-physical risks.

As a result, data breaches and infiltration by hackers may not be as ingrained in the risk mitigation strategy as other threats. This could help to explain why a relatively modest number of businesses worldwide assign a risk profile to their data.

"Cyber is fairly new and has never been part of the established risk organisation," says the VP of technology at a global bank. "The legacy risk organisation never considered cyber scenarios, cyber threat models or cyber-attack scenarios. It's only been recently that we've poured money into a strong cyber group."

2. Passive avoidance: Data owners are resistant to extra work

As with any process-driven internal initiative, organisations are likely to experience resistance from stretched employees who are already busy with their day-to-day tasks. It's not surprising that some try to skip their new responsibilities.

One of the executives we interviewed for this report agrees that many employees will ultimately prioritise their own work. "What you find is that data is all over the place," he says. "Because people have taken exports of data and saved them locally and emailed them to other people – just to get their jobs done."

More worryingly, one of the executives we spoke with has found employees being deliberately misleading in how they rank their data. "We used to leave it to service owners to categorise data, but found that 70% had under-classified to avoid implementing controls," he complains. "So we set up a group that exists to validate responses before they're put into the system."

It is difficult to get the balance right. If you 'over-secure' and enforce some highly rigid controls, you risk creating an unpleasant working culture that leads to attrition. But if you are too lax in implementation, you get 'passive avoidance', where people ignore guidance, or mark something as low priority, to make their lives easier.

3. The right (or most senior) people are out of the loop

If you don't have buy-in at the highest level, any enterprise-wide data initiative is likely to fail. This isn't just because the leadership can provide governance and give the programme its due level of importance – it also ensures that those involved in assessing the data are clear about its wider strategic relevance. Beyond the C-suite, this may also mean bringing in people from all corners of the organisation.

"You need operations, marketing and finance as well as IT," believes Omar. "IT folks ask, 'If an attack happens, what kind of an impact are we looking at?' Operations will tell them about production delays, which could mean more safety stock in the inventory. But then someone in finance will tell them that safety stock kills profits."

Part of the problem is that the drive in recent decades to share knowledge across functional units has made it more difficult to calculate the full impact of a breach. "Understanding needs to come from different units and different functional areas," says Omar.

4. Inconsistency in application

Despite guidance such as the CIA model (as mentioned in Section three) and that provided by the American National Institute of Standards and Technology and other government bodies, it is difficult for large organisations to achieve consistency in how their people think about data. Exacerbating this problem is the fact that the risk attached to one data set may change over time depending on its relevance to current business priorities.

"We have control procedures that provide guidance on what is confidential," says one of the executives we talked to for this research. "But you can never create a list that's going to cover every piece of data. Some people have a hard time figuring out what needs to go in."

5. Underestimating the threat

For some organisations, the principal threat of cyber risk is considered to be the loss of customer data and reputation damage caused by negative media coverage. But this hasn't proven to be as damaging for some companies as originally expected – leading some to downplay the harm that a hack could cause.

Sony is a good example, according to Chris Hankin, Director of the Institute for Security Science and Technology at Imperial College London. "The breaches on Sony had a short-term effect on stock value and customer base," he explains. "But, very quickly, people coped with the fact that their data had been lost. It didn't turn them away from Sony, because they still valued the company and what it did."

Hankin does, however, acknowledge that reputation damage could prove fatal to an organisation such as his own. "It would kill a university if the students stopped coming. The student databases are part of our crown jewels. If we were to get a reputation for not looking after those properly, if we lost large numbers of records, students would lose confidence in us and stop applying and we couldn't operate as a university."

When a breach can be a good thing

Several of our interviewees said that a breach can be a positive experience because it can alert management to the scale of the problem – and highlight weaknesses.

"For those organisations who became victims of cyber-attacks, we noticed they subsequently received funding to develop more secure systems and run additional cyber-security awareness programmes," says A*STAR's Kan.

David Pollino, senior vice president and deputy chief security officer at the US's Bank of the West, believes that some positive outcomes can arise from a relatively minor incident. "You can have a good level of preparation, but until you've been through at least one disaster you will never really know that everything is going to be executed perfectly," he says. "There is always room for improvement."

Our experience corroborates this idea that a minor breach is sometimes necessary to get the board to take greater interest, which in turn guarantees a more structured approach to data security. "Scrutiny is good," says Mike Harris of Grant Thornton Ireland. "You get discipline and structured project management when the board is involved. A challenge for some security projects is that it's an afterthought that IT professionals do when they have time. That changes when the board takes more of an interest."

The way forward: Three steps to better data understanding

Businesses need to get better at understanding their data, but they face many hurdles and challenges along the way. Here, we outline our recommendations to help organisations recognise the importance of their data – and ultimately achieve a more mature approach to information risk management.

1 STEP 1: Clarify ownership: System-wide and data-specific

Information security should be treated like an enterprise-wide, consistently applied risk management issue. This means nominating a system-wide owner – often the chief revenue officer or chief financial officer, if not a dedicated chief information security officer – as well as a 'coalface' owner at the operational level. **It means accepting that your data is a strategic asset that should be risk-rated and incorporated into the risk register.**

"The CFO, above all other C-suite participants, leads cyber-security efforts," says Johnny Lee of Grant Thornton US. "CFOs typically procure insurance products to protect, and they tend to have the most interaction with other executives around enterprise risk."

Pollino at the Bank of the West believes that, at an operational level, the data custodian should be responsible for technical implementation. "They need to dictate the requirements and ensure the right things are happening," he says. "They are also in the best position to say whether you need level one, level two, or level three grades of protection."

One of the benefits of allocating day-to-day responsibility, believes Andrew Harbison of Grant Thornton Ireland, is that data owners are aware that they will be culpable if a breach takes place. "People respond better to personal risk avoidance than they do to direct threats," he says. "If you explain that something is being done to protect both them and the company, and that they will get the blame if they have marked it as low priority to get out of some work, then they will do what you say in order to mitigate themselves against that unfavourable outcome."

2 STEP 2: Embed information risk management 'by design'

Having an enterprise-wide owner of information risk management also makes it easier to ensure that effective data categorisation or assessment are built into projects at the start.

"You have to have security by design," believes Nick Oldham, data security and privacy attorney at international law firm King & Spalding. "Security and privacy are a layer that companies often add at the tail end of a new initiative, which creates problems down the road."

The VP of technology at a global bank is also keen for data security to be embedded earlier on. "What we're pushing is something much more embedded in the development cycle," he says. "We're doing threat modelling, and secure design review, where you iteratively build on the assessment, leading up to a red team adversary-evaluation test."

Cross-functional insight

There are several parts to security by design. One is ensuring that a range of functions are involved in the ongoing assessment and policy-setting process – not just the individual data owners.

"For enterprise risk assessments and impact analysis of cyber-attacks, the whole organisation needs to be involved – and not just the IT department alone," says A*STAR's Kan. "It'll need to be a combination of departments, divisions and business units coming together in a multidisciplinary team to formulate the scenario planning and impact assessments of such incidents."

Destroy as standard

Responsible data destruction reduces the likelihood of a data breach. "You can have a policy around transactional records and sales presentations, and specify how long it is to be kept around," says David Pollino of Bank of the West. "Then you need to take steps to get rid of the data. Things that are kept in email folders, or things that are not under any record hold, would automatically be purged and deleted."

Sunil Chand of Grant Thornton Canada believes that destruction should be built into any agreed handling standards around data. "Your data's usefulness will be dictated by business need, legislation, regulation, and whether you are going through litigation," he says. "The best approach, and it's a simple one, is to have a data destruction policy with accompanying manual or automated controls to enforce as standard unless you still need the information or will need it in the future."

3 STEP 3: Achieve more 'human' communication and training

"Getting your employees to better appreciate the reality of cyber-threats means engaging them on a human level and avoiding technical jargon and 'geek speak'", says Kan. "You have to build IT teams that can bridge the communications gap between business users and technical tools using layman's terms. It's like Human Relationships 101."

For the University of Cambridge's Anderson, successful communication involves better storytelling. "Companies shouldn't be talking about data," he says. "They should be talking about what can go wrong in human terms. The brain is optimised for telling stories and if you start talking about categories of data, you cut people off."

Oldham at King & Spalding agrees, and suggests that companies tailor their messages to talk to individuals' personal concerns and priorities. "There needs to be a fluidity of communication from the board level down to the technical team," he says. "Which is relayed in such a way that general counsels can translate those into legal action items and business-minded executives can translate them into business issues."

Ongoing training

"If a company has to depend on Mike from accounts-payable not clicking a link then that organisation is toast," says Chris Bronk, assistant professor at the University of Houston. "Phishers are so sophisticated. Expecting the people in the organisation to be craftier than criminals is like expecting people to be craftier than car thieves."

Training plays an integral role in improving awareness and resilience among employees, and also helps achieve Kan's 'Human Relationships 101' – especially in ensuring that people start to think about data risk as second nature.

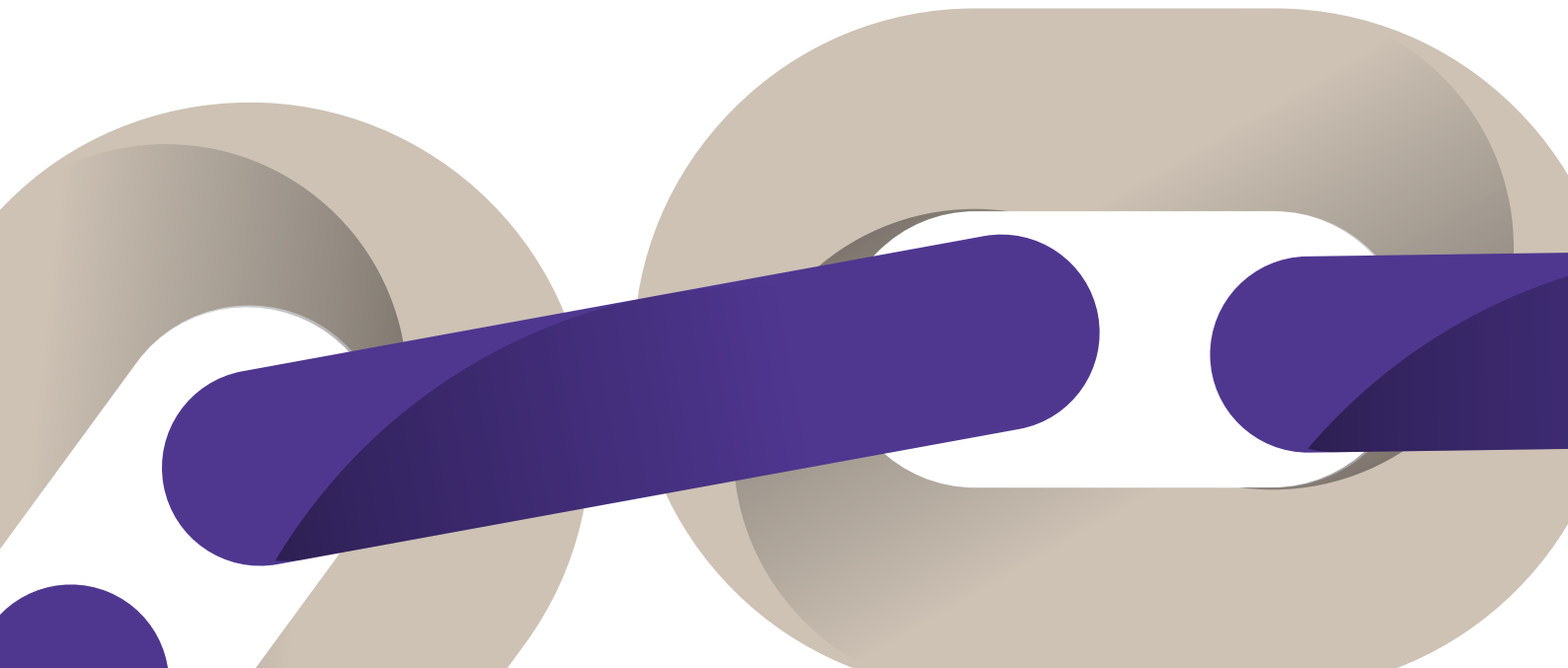
"Any hacker will tell you that the weakest point in a system is the people," warns Grant Thornton's Andrew Harbison.

"So you need to focus on training, training, training. At one organisation I worked with they had green, amber and red classifications for data. But then everything became red eventually, so they had to put in a purple for something even more serious than red. If that happens, you really need to sit them down and explain to them how to rank data correctly."

There are, however, limits to what can be achieved through training. "If you've got people who just aren't good at cybersecurity – and you can't fire them – then your problem never goes away," says Bronk. "You have to come up with some sort of engineering solution that eliminates as many risk factors as possible. This could be a client-based system on top of your email to say, 'Someone just clicked a 'forgotten password' link in an email. Let's trace where it's going, alert the fire log, let's scan those binaries.'"

Beyond 'project fear'

The benefits of better data understanding extend far beyond effective cybersecurity. Anderson says that companies can incentivise their employees to understand their data by pointing to the additional value that can be unlocked during the process. "If there's one thing I've learned over the past 15 years," he says, "it's that cybersecurity is about economics."



In conclusion

In recognition that cyber risk is only going to become more pronounced as new technologies come on stream, most organisations accept that they need to get better at managing the threat.

Cyber risk needs to be approached with an attitude of continuous improvement, and our strongly-held view is that this isn't possible unless you also have a clear and dependable picture of the data you have.

Above all, data should be seen as a critical business asset – yet our research suggests that many organisations do not perceive it as such. They aren't doing enough to understand what they have and how to protect it. Even when they do take steps to improve how they look after their data, they often do so with legacy tools and approaches that are not sufficient to measure, manage and put a price on non-physical risk.

And yet, as we have outlined in this report, a workable and effective approach is certainly within reach. First of all, organisations need to accept that their data is too big – and too important – to ignore.

Beyond this, they need to be pragmatic. If you assume that someone, at some point, will find a way to hack into your systems, you will make sure that your most valuable data remains unassailable.

Ultimately this means understanding what your crown jewels are – depending on your industry, your risk profile and your business goals – and allocating specific controls. It isn't a straightforward activity, or even a finite one, but it is an indispensable part of risk management in the digital era.

“In five years’ time, the infrastructure of computing we have will be used for new and novel security hacks that we can’t imagine”

Chris Bronk, University of Houston

Contact us

We help our clients prepare themselves for cybersecurity threats, ensure ongoing protection, react effectively to attacks and drive change to improve their cybersecurity capability.

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

Sunil Chand
E sunil.chand@ca.gt.com
T +1 416 587 2402
Canada

Mike Harris
E mike.harris@ie.gt.com
T +353 86 855 6740
Ireland

Michiel Jonker
E michiel.jonker@gt.za.com
T +27 113224500
South Africa

Vishal Chawla
E vishal.chawla@us.gt.com
T +1 703-847-7580
United States

Mark Hoekstra
E mark.hoekstra@gt.nl.com
T +31 653978745
Netherlands

Johnny Lee
E j.lee@us.gt.com
T +1 404 704 0144
United States

Andrew Harbison
E andrew.harbison@ie.gt.com
T + 353 1 680 5766
Ireland

Paul Jacobs
(Global leader)
E paul.jacobs@ie.gt.com
T +353 1 6805835
Ireland

Manu Sharma
E manu.sharma@uk.gt.com
T +44 20 7865 2406
United Kingdom

To read more about cyber resilience or how we can help, visit GrantThornton.global

IBR research methodology

The Grant Thornton International Business Report (IBR) provides insight into the views and expectations of more than 10,000 businesses per year across 36 economies. Questionnaires are translated into local languages with each participating country having the option to ask a small number of country specific questions in addition to the core questionnaire. Fieldwork is undertaken on a quarterly basis, primarily by telephone. IBR is a survey of both listed and privately held businesses.

The data for this report was drawn from interviews with more than **2,900** chief executive officers, managing directors, chairmen or other senior executives conducted in between October and December 2016.

Acknowledgements

In addition to the qualitative research above, we worked with Longitude to carry out in-depth interviews with cybersecurity specialists across the Grant Thornton network, as well as external business leaders and board members during early 2017.

We would like to thank the following individuals for giving their time and insight to this report:

- Ross Anderson, professor of security , Computer Laboratory, University of Cambridge
- Chris Bronk, assistant professor, University of Houston
- Tom Faulkner, head of IT production, CMC Markets
- Chris Hankin, director of the institute for security science and technology, Imperial College London
- John Kan, chief information officer, A*STAR
- Nick Oldham, data security and privacy attorney, King & Spalding
- Ayman Omar, associate professor and research fellow at The Kogod Cybersecurity Governance Center, Kogod School of Business at American University
- David Pollino, senior vice president and deputy chief security officer, Bank of the West
- The IT director of an investment management company, who asked to remain anonymous
- The vice president of technology at a global bank, who asked to remain anonymous

About Grant Thornton

Grant Thornton is one of the world's leading organisations of independent assurance, tax and advisory firms. These firms help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice.

Proactive teams, led by approachable partners, use insights, experience and instinct to understand complex issues for privately owned, publicly listed and public sector clients and help them to find solutions. More than 47,000 Grant Thornton people across over 130 countries, are focused on making a difference to the clients, colleagues and the communities in which we live and work.

Grant Thornton

An instinct for growth™

grantthornton.global