IRM INFORMATION RISK MANAGEMENT
•ALTRAN GROUP

2019 REPORT

RISKY BUSINESS

ALTRAN

SECURE CYBER **UNLOCK OPPORTUNITY**

IRM**SECURITY**.COM

TABLE OF CONTENT

WHAT'S THE LATEST IN CYBER

Before we dive into the Risky Business 2019 findings, let's take a look at the cybersecurity landscape this year.

$700m

Equifax was fined $700 million following their wrongdoings in protecting data belonging to over 147 million customers. This followed the widely-reported British Airways and Marriott data breach fines, not to mention the notorious Facebook incident.

7 days

The amount of time it took 34%* of businesses hit by a malware attack to regain access to their data. One of the largest attacks this year was the Norsk Hydro ransomware attack in March, paralysing their computer networks and costing them a reported $52 million in Q1 of 2019.

54%

New mobile malware variants increased by 54% since 2018**, illustrating that cybercriminals are targeting the ever-growing number of mobile devices.

Sources: *Kaspersky.co.uk
** Symantec's Internet Security Threat Report

THE RISKY BUSINESS OF CYBERSECURITY.

Welcome to IRM's Risky Business Report

If you haven't heard of Risky Business before, it's an initiative from Information Risk Management (IRM) which involves surveying cybersecurity and risk management decision-makers. Topics in the survey this year included cybersecurity management challenges, perceived biggest threats, security maturity levels and future opportunities.

After analysing the results from 2019's survey - which ran from July to September – we compiled this report to deliver the highlights back to the industry. Over 83% of survey respondents are cybersecurity budget holders (for example, CISOs, Risk Managers, Security Managers) spread across seven sectors including automotive, communications, energy, finance/public sector, software/internet, transport and pharmaceuticals. You can find our methodology on Page 30.

We hope that the key findings delivered in this report will resonate with you and that any learnings will assist you in developing and improving your future strategy.

Executive Summary

With a clear divide in management surrounding the priority of cybersecurity, the report shows that the unwillingness to invest in cybersecurity implies that most senior managers are failing to understand and recognise its value.

Cybersecurity budgets are focusing on the basics - perimeter security and people - educating and raising awareness of security risks with a preference towards internal training. Despite this investment in training, organisations still see employees as generating the highest level of risk.

Security teams and managers continue to feel the pressure from all angles, including the burden of immature security teams and frequent questions from executives when they struggle to translate audit compliance results. Not to mention keeping abreast of legislation, such as the NIS Directive/NIS Regulations.

When planning for the worst, the survey found that approximately 93% of organisations have an incident management plan and the ones who don't noted it was mainly down to the organisation's lack of security awareness. Looking to the future, 5G and AI are at the top of the agenda, with an overwhelming majority recognising both developments will have an impact on their cybersecurity strategy.

KEY FINDINGS OF THE REPORT

HUMAN ELEMENT - Organisations think employees generate the highest risk, with existing staff seen as the most risky, rather than disgruntled leavers or new staff.

SUPPLY CHAIN - There's a large variation in the regulation of assurance activities, with 9% of organisations unaware of how many third parties they share data with.

FUTURE PROOFING - 5G and AI will play a big part in future strategy; creating challenges and impacting cybersecurity strategy for the majority of respondents.

The Future of Risky Business

As traditional industries move towards digital transformation to innovate and remain relevant, the traditional IT security discipline is fast-merging with engineering disciplines. IT professionals are increasingly having to collaborate with operational technology (OT) designers and engineers. They combine forces in an IoT-enabled world to optimise business processes and incorporate cybersecurity at every step. IRM's Risky Business Survey and Report will evolve in future years to encompass the IT/OT convergence, so we've highlighted future cybersecurity trends as Industry 4.0 becomes mainstream.

DevSecOps - Organisations redesigning legacy systems are starting to recognise that security reviews can no longer be performed during the final stages of the development lifecycle. The DevSecOps approach introduces the idea that everybody is responsible for security, integrating security best-practice into the DevOps pipeline to ensure that organisations can confidently bring software to market with security assurance in place.

Leading Industries – Whilst many industries lag behind, automotive is leading the way with digitisation, with the connected car industry expected to grow by 270% by 2022*. Factors including the affordability of RFID technology and cognitive computing and AI developments have convinced car manufacturers to invest in connected vehicles and factories. The impact of this trend? Vast amounts of sensitive data stored in the cloud which makes automotive more susceptible to cybercrime than ever before.

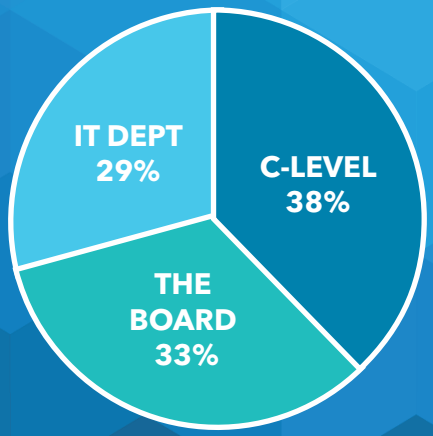
Industry Disruptors – There's no time like the present for organisations to grab hold of the latest technology to make an industry impact, whether it's Uber changing the way we take taxis, or Monzo making waves in online banking. But what does the future hold for industry disruptors? We will be forced to rethink existing operations and perhaps we will begin to question the power held by data-hungry organisations...

Internet of Things (IoT) – IoT manufacturers receive large investments to quickly drive a minimal viable product (MVP) to market to maximise profit. The development of IoT products lacks a systematic approach to cybersecurity. With little or no thought towards security during the dev cycle, investments are soon negated if the product falls victim to a cyber-attack. Will these businesses begin to recognise this, or will the MVP approach continue?

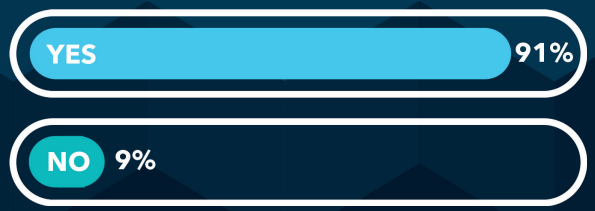
*Source - Internet of Business

CYBERSECURITY: A C-SUITE LEVEL CONCERN.

Q1: Where does your cybersecurity function report to?



Q2: Is the increased level of cybersecurity awareness at C-Level translated into their decision-making?



LET'S EXPLORE...

A balancing act

IRM's last Risky Business Report focused on the Board finally realising the importance of cybersecurity and 2019's findings support this idea even further.

An overwhelming 91% of respondents agree that the increased level of awareness around cybersecurity at the top of the business continues to be translated into wider business decisions. Specifically, respondents note that there has been a noticeable rise in accountability, where business leaders are beginning to recognise and understand their responsibilities. Whether these are legal obligations, such as GDPR, or ethical responsibilities to customers and suppliers, most respondents feel they are getting more support.

On the other hand, many respondents are facing a divide in management. A key theme being that previous managers tend to have little concern about cybersecurity, but the introduction of new management has resulted in a commitment and willingness to pay for prevention and protection against cyber-attacks.

Despite the increased desire to invest in cybersecurity, the cost is a recurring issue. Many respondents highlight that the C-Suite is still not as security-aware as it needs to be. Most decisions tend to lean towards what the accountants require, rather than the safest decision for the business. This response indicates a lack of understanding of the true financial and reputational impact that can occur when an organisation experiences a cyber-attack.

THE BUDGET-HUNGRY AREAS OF CYBER.

Q3: In the last year, which areas of cyber have you invested most of your budget in?

LET'S EXPLORE...

Protecting the castle

From the diagram, you can see that the most popular area of investment over the last year is "perimeter" security. According to our respondents, their budgets are mostly being spent on firewalls, strengthening endpoint protection and introducing anti-spam security.

This is an interesting discovery considering there has been much discussion over the years about whether the concept of a perimeter in cybersecurity is even still valid. The increasing use of 'bring your own device' and cloud computing means that the traditional view of a 'barrier' around a static business environment is likely to have disappeared. Whilst it's still important to have layered controls in place to protect your organisation, it is clear that there are other areas of security which also require investment.

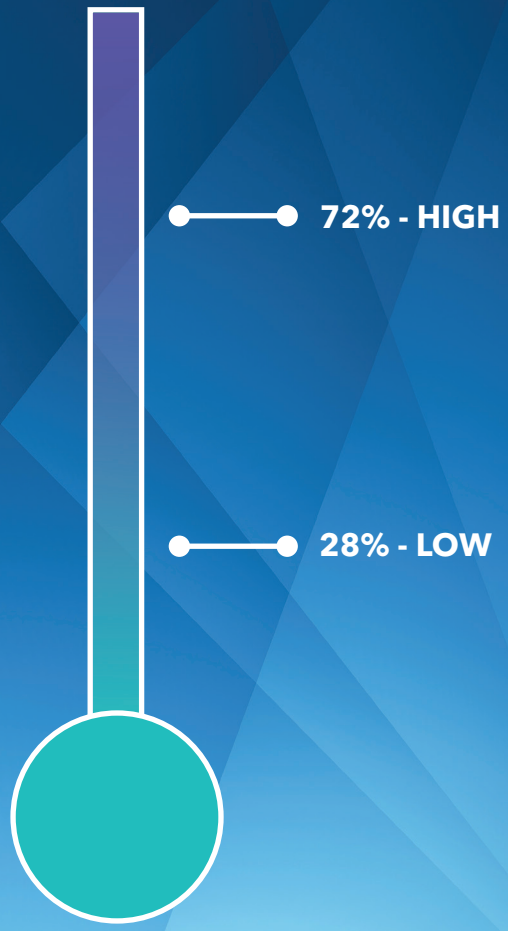
Many organisations have turned their focus to solving "the people problem", as one respondent describes it. A lot of organisations' recurring spend is on educating staff. This investment makes sense considering you can have the best anti-spam protection in place, but if an employee clicks on a malicious link due to their lack of cybersecurity awareness, you've potentially got a much bigger problem.

Other common expenditure areas include investing in cloud security and focusing on SOC capabilities. The popularity of developing cloud security is no surprise considering that a recent survey* found that 50% of organisations had a 'cloud-first' or 'cloud-only' policy. Are these businesses conducting cloud security assessments on implementation and considering the risk impacts of these changes?

Source: *North Bridge Cloud Computing Survey

THE PRESSURE CONTINUES.

Q4: How would you rate the pressure from stakeholders to understand how your company is managing cybersecurity?



LET'S EXPLORE...

The hot subject on everyone's lips

Over two-thirds of Risky Business respondents rated the pressure from stakeholders high, as they seek to understand the status of security within the business.

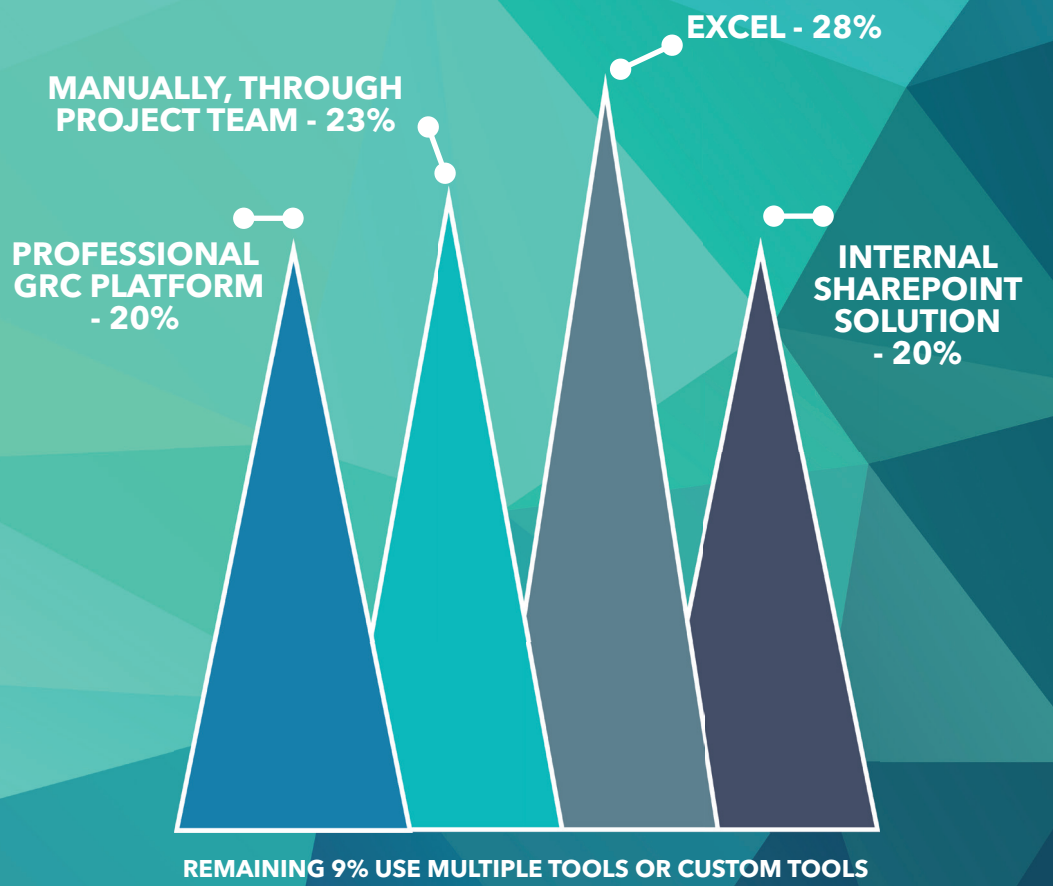
In particular, some respondents point towards the spike in pressure when it comes to compliance audits. More specifically, having to spend considerable amounts of time responding to the audits as well as having to explain the outcomes to stakeholders. There is also little surprise to learn that internal politics is still a pain point for security managers. There's a clear indication that areas of the business which are less security mature require the more-developed departments to constantly share information with them to obtain a sense of inclusion.

Why are stakeholders ramping up the pressure on security decision-makers? The increased media coverage of hefty fines for data breaches, like those from British Airways and Equifax, are likely to be contributing to the increased awareness of cybersecurity best practice. Whilst this media coverage can help you raise the profile and importance of security investment, it seems to be leading to increased scrutiny of current security practices and future plans. As well as the media, the supply chain is heightening tensions. Whether customers are concerned over the protection of their personally identifiable information, or suppliers are conducting third party assessments, these varied requirements are adding to the pressure.

Rather than allowing the Board to push a tick-box approach to becoming compliant and avoiding fines, you should work *with* them. Collaboratively, you can define key objectives, allowing you to build a thought-out cybersecurity strategy.

EXCEL IS STILL KING, BUT GRC PLATFORMS GAIN MOMENTUM.

Q5: How do you manage your cybersecurity efforts?



Professional platforms on the rise

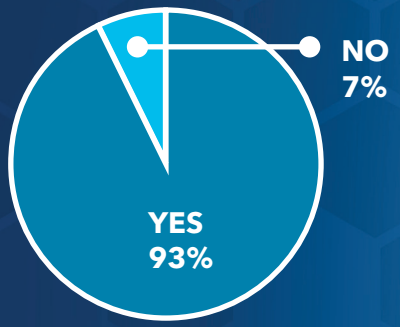
This question attracted the biggest mix of responses in this year's survey, showing that there is still a huge variation in how you manage your cybersecurity and risk management efforts.

Over a quarter of respondents, however, state that Microsoft Excel is still their main tool to manage their governance, risk and management (GRC) programmes. This comes as no surprise to IRM, as we work with many clients who often opt to manage their GRC efforts in spreadsheets. Whilst this result is not unexpected, we continue to be concerned as Excel is an outdated GRC management tool. It requires hours of time to enter data, create reports, correct errors and chase manual tasks across the business, leaving you with little time to put effort into facilitating effective risk management mitigation and remediation programmes.

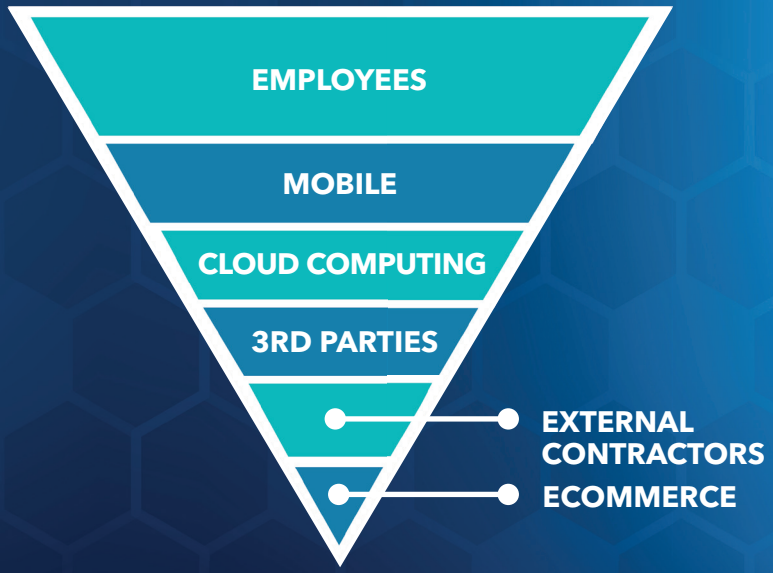
Needless to say that some organisations have moved away from this method of management. Some organisations are opting for all-in-one GRC platforms, whilst others are choosing software that focuses on one type of challenge (such as risk management) or 'point' solutions designed to cover particular types of compliance, such as the GDPR. These software tools can help create a much greater integration and increase visibility when governing risk. Most importantly, it can help you create pervasive accountability and responsibility for managing risk by delegating risks to relevant stakeholders, not to mention the valuable time-saving element.

IS CYBER JUST A PEOPLE PROBLEM?

Q6: Have you undertaken a threat assessment?



Q7: What do you consider as the most vulnerable area of security?



LET'S EXPLORE...

Knowing where the cracks will appear

The results show that over 93% of respondents have conducted a threat assessment on their organisation, but a worrying 7% have not. Whilst this isn't a large figure, it raises concerns that some security functions may be operating and implementing strategies without even understanding their true threat landscape.

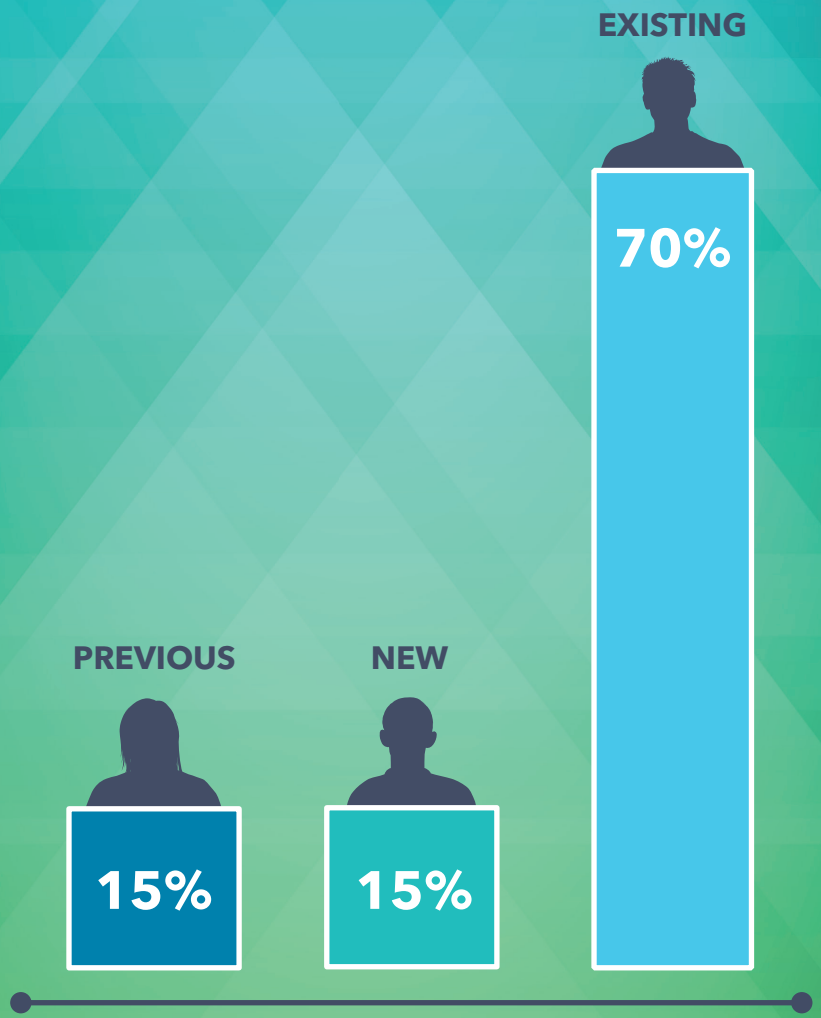
When delving further into the threats, we discover that respondents feel that 'employees' prove to be the biggest security threat. In comparison, third parties are only considered the fourth biggest threat.

Is this perception skewed? You could assume that, because employees are within the control of a business, it would be easier to manage the threat level. Security awareness training is becoming more and more popular. Whether it's delivered online or face-to-face by internal experts or an external agency, it should be a fairly simple process to put your people through their paces when it comes to security awareness. Let's compare this to a third party, such as a cloud-based data storage supplier. Apart from being able to conduct risk assessments, how much can you really trust your third parties?

Perhaps some organisations have resigned themselves to the fact that it will always be notoriously hard to monitor and manage the risks of their supply chain. Whilst it's fairly obvious that third parties are likely to cause the same (or higher) level of risk than your employees, the statistics still show that organisations consider their 'people' as generating the most risk. This is explored further in the next question.

85% SEE EXISTING STAFF AS INTRODUCING THE GREATEST RISK.

Q8: Which type of employee do you think introduces the greatest risk into your organisation?



LET'S EXPLORE...

The inevitability of human error & malicious intent

So the survey responses so far tell us that most organisations consider employees as one of their biggest threats, but what *type* of employee?

Results showed that around 70% of respondents feel that existing staff (including those who work remotely) pose the biggest threat, compared to 15% for new employees and 15% for previous employees.

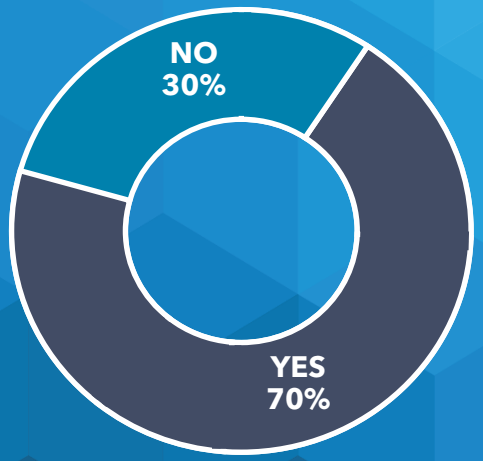
The results are to be expected when we think back to examples such as Morrison's 2014 data leak. This is when a disgruntled existing employee (with access to employee data) leaked the personal details of over 100,000 staff, including salary and bank information. Despite having appropriate measures in place to protect the data of its employees, The High Court and Court of Appeal both found Morrison's to be liable for the actions of the employee and the subsequent data breach.

What exactly does this mean for employers? Firstly, it means that employers are at a much higher risk of becoming responsible for the actions of their employees, placing more emphasis on the need for company policies and security awareness training. Secondly, it indicates that organisations should implement substantial and appropriate vetting and monitoring processes during the recruitment process.

Despite efforts made, however, no matter how much time and money you put into training employees on legislation, such as the GDPR and how to protect personal data, it all comes down to trust. You can inform and educate employees on the value of personal data and the legal obligations surrounding it, but when access to information is so readily available, you must really consider who you put in positions of responsibility.

A WAKE-UP CALL TO THE NIS DIRECTIVE.

Q9: Are you aware of the NIS Directive/NIS Regulations?



Q10: Have you implemented the necessary changes in line with the NIS Directive/NIS Regulations?

LET'S EXPLORE...

In the shadows of the GDPR

We were interested to understand the overall awareness of the NIS Directive to date – a piece of EU legislation setting a range of network and information security requirements for Operators of Essential Services (OES) and Digital Service Providers (DSP). For those in the UK, this Directive was enacted in UK law as the Networking and Information Systems Regulations 2018 on the 10th May 2018.

The results show that 30% of organisations are unaware of the legislation. This could be down to the huge level of noise around the General Data Protection Regulation (GDPR), which has led to an obvious shortfall in attention around the NIS Directive. Out of the 70% of respondents who were aware of the legislation, over a third have failed to implement the necessary changes in line with the regulations and only 39% are confident that they are compliant in this area.

If organisations are aware of the regulations, why aren't they complying with the standards? Perhaps they are not aware that non-compliance against the NIS Directive can equate to a maximum £17m fine, enough to cripple a business.

Perhaps there is confusion around exactly what it means to be an OES or DSP and organisations are unsure of their responsibilities and actions required. Lack of resources, tools and budget is most likely the reason for the NIS Directive falling behind as a priority, but it will certainly need assessing by organisations who haven't done so already.

9% OF RESPONDENTS DON'T KNOW HOW MANY THIRD PARTIES THEY SHARE DATA WITH.

Q11: How often do you carry out third party assurance activities?

LET'S EXPLORE...

Communicate, communicate, communicate

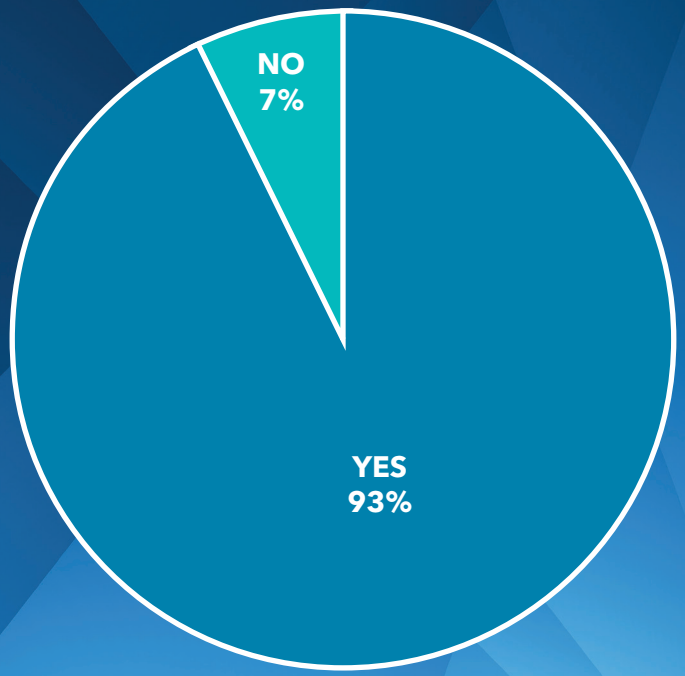
The results show a huge variation in regularity of assurance activities against third parties. In general, it seems that activities *are* taking place, but not regularly. Most importantly, 9% of respondents don't know how many third parties they share data with, indicating that these organisations are not checking the compliance or security practices of their third parties.

Not participating in assurance activities like these can increase your security threats considerably. As an organisation that is likely to be part of a wider supply-chain, you are only as strong as the weakest link in your chain. It's common for smaller contractors to have less stringent controls in place, therefore pinpointing them as a particular area for concern. If there is regular network access between third parties or information and data is being shared, assurance activities are even more vital. It's worth asking yourself, are you aware of the security posture of your suppliers, how your data is being handled and are they sub-contracting work out entirely? Furthermore, are these activities carried out on a regular basis? From the offset, build trust with your supply chain and clearly communicate your minimum security requirements expected.

Best practice advice from the UK's National Cyber Security Centre states that there are four stages to consider when assessing your supply chain: understanding the overall risks, establishing control, checking your arrangements and improving and maintaining security as your supply chain evolves.

IF YOU FAIL TO PLAN, YOU PLAN TO FAIL.

Q12: Do you have an incident management plan in place?



Know the lie of the land

An overwhelming 93% of organisations who answered the survey said they have an incident management plan in place. But what about the other 7%?

Respondents who don't have a plan in place noted that there is an overall lack of awareness in the organisation. We can assume that, despite the enthusiasm from risk and security managers to implement plans in the event of a cyber-attack or breach, the lack of support from higher management and/or the Board creates a huge barrier.

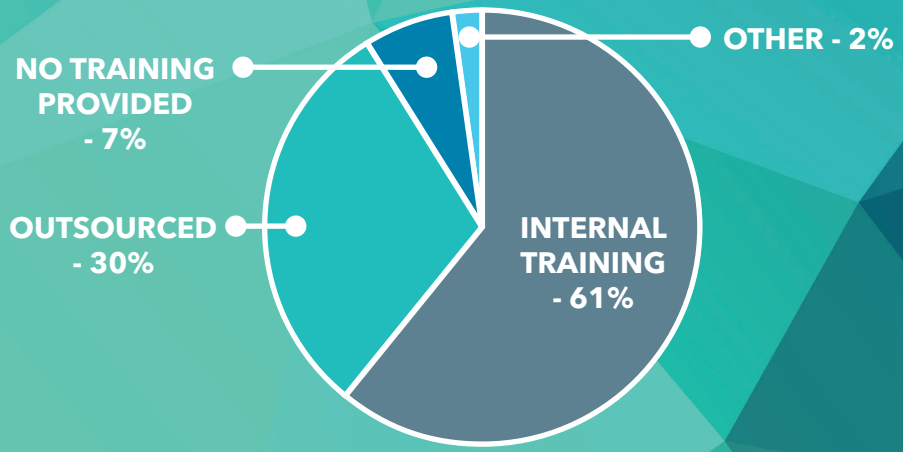
There may also be a case of "it won't happen to us" attitude amongst organisations who don't have an incident response plan in place. This year has shown that even the most unlikely organisations can be targeted by a cyber-attack, such as the theft of audio files from a radio station in Missouri in August. Whilst it's always easy to assume that your organisation has nothing of value to a cybercriminal, you should assess your threat landscape.

You may not be a target of nation state cybercriminals, but you could be the next on the list for a tech-talented script kiddie hoping to make a quick buck on the Dark Web. A threat landscape analysis exercise will help you understand your overall security risks before preparing an appropriate incident response plan.

To put the importance of an incident response plan into perspective, research from IDC shows that, in an attempt to protect organisations from an attack, global spend on cybersecurity solutions is set to exceed $103 billion in 2019 alone, an increase of 9.4% from last year.

RESEARCH & DEVELOPMENT IN CYBERSECURITY.

Q13: What sources do you use for your cybersecurity training?



Q14: What research resources do you utilise?

LET'S EXPLORE...

Be aware of the dark side

A majority 61% of respondents said that they mostly provide internal training to staff to increase their knowledge and understanding of cybersecurity. This is compared to 30% who utilise outsourced training, and 7% who offer no training programme at all.

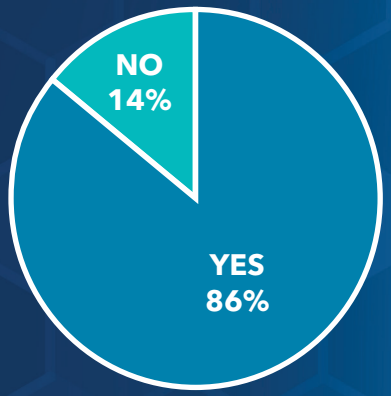
If you have access to tools such as eLearning platforms or intranets, facilitating cybersecurity training internally can be quite easy. As a minimum, most organisations will offer courses covering the basics of cybersecurity, data protection and how to spot malicious emails. But is this enough? And is there bias when curating and distributing training internally?

Although cybersecurity managers have a lot of knowledge in their field, sometimes you can benefit from receiving the support of outsourced training to provide a wider view of the organisation's threat landscape. Some training consultancies can bring threats to life for employees. For example, completing online training about not clicking on malicious links can be informative, but witnessing a live hacking demonstration from a phishing email may emphasise the learning point even more.

When it comes to researching the latest cybersecurity trends and threats, we asked respondents what they use as their main source of information. Whilst there was a variety of answers, there was a clear preference of attempting to learn directly from the threat actors. For example, many respondents noted that they look at the dark web, whilst others join hacker communities and read industry reports to discover the latest vulnerabilities and attacks they need to be aware of.

THE IMPACT OF AI - ARTIFICIAL INTELLIGENCE.

Q15: Do you see AI having an impact on your cybersecurity strategy in the next 5 years?



Q16: What are the top three AI applications you would consider implementing as part of your cybersecurity strategy?

#1	NETWORK INTRUSION DETECTION & PREVENTION
#2	FRAUD DETECTION
#3	SECURE USER AUTHENTICATION

LET'S EXPLORE... WITH DAVID HUGHES
MSci MBA (TECHNOLOGY MANAGEMENT) PhD

(ANALYTICS SOLUTIONS LEAD, TESSELLA - PART OF ALTRAN GROUP)

The rise of the robots

86% of respondents affirm the increase in demand for AI in cybersecurity systems, with the top application aiming to detect and prevent network intrusion. This is where the AI system is trained to learn normal behaviour based on the data available to it. Once trained, it can continuously monitor unusual behaviour and flag for attention. Deployed correctly, it can shorten the response time and reduce (but not eliminate) the effort needed by security analysts, allowing them to be more effective. However, these approaches are not foolproof and care needs to be taken to ensure you can trust the results.

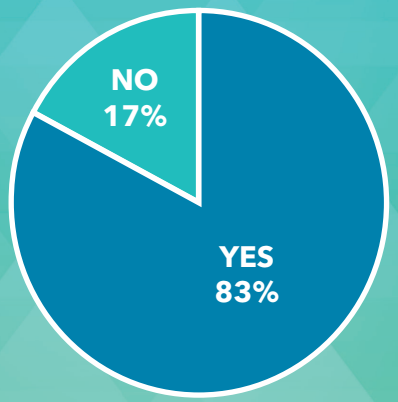
AI is fundamentally based on behaviour patterns, so unusual but legitimate behaviour is likely to set off a false alarm and subtle attacks may be missed. Ensuring training data is representative will improve accuracy, and multi-layer defence will help to ensure that threats missed by AI will still be caught. Without suitable context or explanation, an alert from an AI system may be difficult for an analyst to take action on, meaning the interaction between the AI and the analyst is just as important.

Production systems based on AI also introduce new security aspects. For example, deep learning systems can extract information through specifically created queries or even through normal use. Systems with a public interface or API access are potentially vulnerable in a way that a rule-based system is not. Coupled with the tendency of these systems to inadvertently memorise facts, this becomes a privacy and IP risk that needs addressing through careful system design and monitoring.

AI in cybersecurity is a double-edged sword. It can provide many companies with the tools to detect fraudulent activity on bank accounts, for example, but it is inevitably a tool being used by cybercriminals to carry out even more sophisticated attacks. In September this year, criminals used voice-mimicking software to imitate the speech of an executive in order to convince his subordinate to send hundreds of thousands of dollars to an outsider's account. In what is now being dubbed as one of the world's first publicly reported AI cybercrime heists, we are likely to see more of this occuring as the technology develops.

IS THE MARKET READY FOR 5G?

Q17: Do you think 5G developments will create cybersecurity challenges for your organisation?



Q18: What are your top three 5G security challenges?

#1	GREATER RISK OF ATTACKS ON IoT NETWORKS
#2	A WIDER ATTACK SURFACE
#3	A LACK OF SECURITY BY DESIGN IN 5G HARDWARE AND FIRMWARE

LET'S EXPLORE... WITH SHAMIK MISHRA

(ASST. VICE PRESIDENT - RESEARCH & INNOVATION AND GROUP CHIEF ARCHITECT, COMMUNICATION INDUSTRY - ALTRAN GROUP)

Secure 5G implementation is paramount

We asked a similar question about 5G, where 83% of respondents agree that 5G developments will create cybersecurity challenges for their organisation. When asked what their top 5G challenges are likely to be, the top three areas are 1) a greater risk of attacks on IoT networks, 2) a wider attack surface and 3) a lack of security by design in 5G hardware and firmware.

Some respondents are also concerned by the existing 4G challenges carried forward, but the acceleration to market of 5G and lack of security considerations is causing concern. Tom Wheeler and David Simpson from The Brookings Institution said: "to build 5G on top of a weak cybersecurity foundation is to build on sand".

Shamik Mishra, Altran Group, confirms that 5G produces a larger attack surface as more distributed network data centres (called near and far edge) get deployed. The deployment will be much more dense, the computer platforms will get distributed and therefore the attack surface is large. The vulnerabilities in 5G appear to go beyond wireless, introducing risks around virtualised and cloud native infrastructure. In order to drive 5G deployments, a secured infrastructure strategy is required and white box/disaggregated hardware will be critical to lower the total ownership cost. However, it's not known if such hardware has the right security solutions, so implementing device security practices will be critical to making this model work.

5G will also require more third party involvement. 5G is the last chance for the operators to counter the "over the top" providers. Edge Computing and 5G network clouds are going to be important for executing 5G use cases. These use cases will be implemented in the usual B2B models that cloud companies (like AWS, Google etc) utilise today. This means that lots of new and third party applications will be brought in, which automatically means more vulnerabilities (through rogue applications or vulnerable non-secured software).

Mishra adds that data protection should also be considered, as confidentiality protection for both consumers and application providers is a critical aspect for operators to address with 5G technology. Looking to the future, the successful and secure implementation of 5G will require commitment and collaboration from businesses and governments alike.

METHODOLOGY

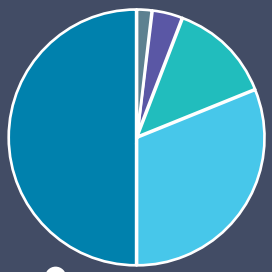
Primary Survey

We conducted a focused survey between July and September 2019 with 50 global enterprises spread across numerous industries and geographies, detailed below. 83% of respondents are cybersecurity budget-holders (including CISOs, Security Managers and Risk Managers).

BY INDUSTRY

- FINANCE/ PUBLIC SECTOR - 34%
- OTHER - 32%
- SOFTWARE/ INTERNET - 10%
- TRANSPORT - 6%
- AUTOMOTIVE - 6%
- COMMUNICATIONS - 6%
- ENERGY - 6%

BY GEOGRAPHY



- NORTH AMERICA - 50%
- EUROPE - 31%
- ASIA - 13%
- SOUTH AMERICA - 4%
- AFRICA - 2%

BY CYBER BUDGET

- UNDER £50K - 20%
- £51-200K - 20%
- £201-500K- 18%
- £501-1M - 16%
- £1M + - 13%
- NO BUDGET - 13%

ABOUT INFORMATION RISK MANAGEMENT (IRM) AND ALTRAN

About IRM

Founded in 1998, IRM provides visibility and control across entire cyber landscapes by combining more than two decades of consultancy with advanced technology. As Altran's World Class Center for Cybersecurity, we cover everything from cybersecurity governance to automated threat intelligence.

Enabling organisations to comply with ever-evolving standards, legislation and regulation is a key objective for IRM. As cybersecurity experts, we collaborate with manufacturers, suppliers and regulators to stay abreast of the latest R&D.

About Altran

Altran ranks as the undisputed global leader in Engineering and R&D services (ER&D), offering an unmatched value proposition to address their transformation and innovation needs. Altran works alongside its clients, from initial concept through industrialisation, to invent the products and services of tomorrow. In 2017, Altran generated revenues of €2.9 billion, with some 45,000 employees in more than 30 countries.

Why work with IRM?

- **Altran's World Class Center for Cybersecurity** – working across the globe with cybersecurity experts in the operational technology fields to offer a unique perspective and set of skills to combat security testing in Industry 4.0
- **Over 20 years' experience** - IRM combines more than two decades of consultancy with advanced technology to support organisations on every step of their cyber maturity journey
- **Highly accredited consultancy** – government grade certifications and accreditations - IRM is in a strong position to offer security testing services
- **360° solution –** SYNERGi our award-winning GRC platform maintains and reports on compliance, including a unique Pen Test Portal

IRM INFORMATION RISK MANAGEMENT
• ALTRAN GROUP

Think cyber.
Think security.
Think data.

For more information regarding the Risky Business Report, or our cybersecurity services please contact hello@irmsecurity.com

VISIT **IRMSECURITY.COM**
TEL **0044 (0) 1242 225 200**

SECURE CYBER UNLOCK OPPORTUNITY.