EXECUTIVE SUMMARY

Now, more than ever, boards are taking an interest in and ownership of cyber security. Recent high-profile security breaches have shown how they are not only an operational issue, but can also cause long-term reputational damage, lead to revenue loss and incur significant fines from regulators.

GDPR and comparable industry regulations have further sharpened focus in the boardroom, as highlighted by 72 per cent of this year’s respondents being concerned with the detrimental effects resulting from data loss. The burden of responsibility faced by boards filters right down through the supply chain, emphasising the importance of robust due diligence right through the procurement process. Sixty-eight per cent of this year’s respondents have changed a procurement decision as a direct result of cyber security issues.

Organisations face increasing pressure to deliver secure systems and data protection, coupled with industry-wide skills shortages and boards are thinking hard about where to invest. GDPR is still taking up the lion’s share of investment funds but is closely followed by incident response and training programmes. Boards appear to be looking more closely at the business processes that are in place to mitigate a breach and increase awareness of cyber security issues throughout the enterprise. The use of managed security service providers (MSSPs) has almost doubled since the last survey and suggests that third-party vendors are picking up operational business with scarce in-house resources being targeted to the businesses’ primary areas of focus.

There is no let-up in the demand for skilled cyber security personnel. This year’s research shows that security operations skills are the most sought after. Perhaps in part due to a shortage of suitable talent and in part down to a maturing market, our research shows that experience and knowledge are growing in importance over the box-ticking of industry accreditation.

James Walsh – CISMP
Head of Security Practice
Harvey Nash

Andrew Samsonoff
CEO
Invinsec

Please note: For the purposes of the survey, cyber security is defined as an umbrella term encompassing information security and information assurance.
INVESTMENT

With its introduction in May 2018, it is unsurprising that the most prominent investment priority this year has been taken up by GDPR – with almost two in three (63 per cent) listing it as a focus. More interestingly, this year’s research shows that the biggest increase in investment is for managed security service providers (MSSPs); since our 2016 research the proportion of organisations investing in this area has grown from one in ten to almost two in ten (18 per cent). As the competitive landscape for all organisations becomes harder to navigate, businesses need to improve both their output and processes, and this is where investment in outsourcing providers can prove invaluable. Just as major data centres were initially developed in-house then moved to outsourced providers before businesses embraced cloud services, it appears likely, through both quantitative and qualitative research, that security operations (SO) are following a similar life cycle. Further analysis on the drivers around outsourcing is available on page 7 of this report.

Organisations are favouring investment in outsourced provision over hiring

Security incident and event management (SIEM) is also receiving more interest from the board with investment in cyber incident response increasing by 46 per cent in 2018 compared with the last time we asked the question. However, only 37 per cent of respondents state that they are investing in the tools associated with this task which might also indicate a rise in outsourced provision. A corresponding fall in investment associated with hiring (down 35 per cent) also corroborates this. If SO and SIEM are outsourced effectively, IT teams will have more time to develop and improve processes and applications for the business, leaving capable third parties to deal with the day-to-day tasks around cyber security.
RESPONSIBILITY & OWNERSHIP

Since the TalkTalk breach in 2016, there has been a small but steady increase in the degree to which boards feel engaged with cyber security and within larger organisations there are questions increasingly being asked about the advisability of CIOs having autonomy and self-regulation from a security perspective. Respondents stating that their board is ‘Very well informed’ about cyber security has increased by 24 per cent in 2019 compared with 2016. But while cyber security is on the agenda at board meetings, it does not follow that board members will understand how to tackle the issue. Most board members have expertise in other forms of risk, but not in how to protect corporate assets from nation-state attackers and organised gangs of cyber criminals. It is essential that boards focus on removing the obstacles that prevent their organisations from developing a culture of proactive security. Without support from executive management and the board, companies are unlikely to develop strong cyber security practices.

Responsibility for cyber security has shifted

Where does the overall responsibility for cyber security sit within your organisation?

Apart from the relatively small increase in board responsibility (up 4 per cent), there has been a shift away from responsibility lying with IT, Governance and Risk management departments. This year’s research clearly shows significant drops with, for example, only 18 per cent of respondents stating that responsibility lies within IT in comparison with 36 per cent in 2016. This suggests that organisations are recognising the need to have a check and balance between IT and Security, and also that the focus on GDPR has shifted some of the emphasis towards Data Protection Officers to shoulder the burden as a dedicated role. Outsourcing to MSSPs has certainly been a factor in workloads reducing, but responsibility cannot be shifted outside the organisation. It is clear that a major shift in ownership has occurred.

Outsourcing

A surge in cyber threats and the administrative burden involved in staying on top of data security place pressure on organisations that wish to avoid serious data breaches and the associated reputational damage and operational disruption. Given ongoing cyber skills shortages, organisations are forced to look increasingly at outsourced providers and technologies that can help them neutralise and remediate cyber threats in the timeliest way possible. This is evidenced by the investment plans highlighted on pages 4 and 5.

Lack of in-house skills remains top reason to outsource

What are your primary reasons for outsourcing elements of cyber security?
This year's research shows that while the outsourcing of many areas of security operations (SO) has held steady over the course of the last three years, there are some notable exceptions. Just less than a quarter (22 per cent) of respondents are now outsourcing incident management and response in comparison with only 8 per cent in 2016. This is a significant increase. This year, a third of respondents are outsourcing their network security and firewall management compared with 22 per cent in 2016, which also represents a notable increase. Training and awareness around SO is another growing area where respondents tell us that they are increasingly outsourcing, up 23 per cent compared with 2016. All of these measures relieve headcount pressure within the organisation and enable more value-add activities to be performed by precious headcount.

Incident management and response has shifted to MSSPs

Have you outsourced any element of cyber security?

Security in the Supply Chain

The 2017 ‘NotPetya’ campaign began with an extremely effective supply chain attack, which had disastrous consequences for Ukraine's national bank, airport and government departments. It went on to infect machines in a staggering 64 countries. No wonder then that 93 per cent of our respondents’ organisations consider cyber security an important factor for procurement. It is equally unsurprising given that many regulations such as GDPR, and regulators including the FCA, make it clear that organisations own the risk to their data throughout their supply chain.

Overlooking the cyber resilience of suppliers can dramatically increase an organisation’s vulnerability. Our research shows that more than two-thirds (68 per cent) have changed a procurement decision based on security considerations, highlighting encouraging levels of due diligence being undertaken.

Do you consider cyber security when making procurement decisions for new suppliers?

Cyber security in the supply chain is not limited to initial due diligence during procurement but must be embedded in the entire supplier management life cycle. Regular review of existing suppliers provides greater assurance to business about their cyber security risk profile.

Hargobind Singh Ahluwalia, Group Information Security Manager, CPP Group
Security operations must develop a much deeper understanding of how their businesses are changing. Cloud computing is underpinning wholesale digital transformation for companies and creating a significant shift in operational risk. With the integration of cloud services now a standard part of the business landscape, we asked our respondents about whether this made it more difficult to implement effective cyber security. More than three-quarters feel that cloud either made it easier to implement security or had no direct impact on vulnerability.

A quarter of respondents feel that cloud services make cyber security easier to implement.

In your view does using cloud services make cyber security a harder or easier task?

Phishing and social engineering attacks remain at the top of the attack type leader board with 61% of all respondents having suffered from them. Data loss (33% per cent) and service interruption attacks (39 per cent) have almost doubled since 2016.

Which, if any, of the following have you suffered in the past year?

Phishing remains a primary attack vector for all organisations. Given the low investment for this type of attack required for cyber criminals, it’s an obvious first choice tool in their weaponry. It is great to see this report reflect a 16% reduction in phishing and social engineering since 2016. It means that investments in defensive security technology are paying off.

Katy Hinchcliffe, Head of Cyber Security, Littlefish Ltd
Vulnerability management is hard. It’s the constant race against exploits in known holes in your technology. A third of respondents state that attacks affect their revenue and profits. However, the fastest-growing effect of security breaches is a loss of supplier confidence with almost double the amount of respondents citing it as an effect compared with 2016.

### Loss of supplier confidence is fastest-growing impact result

<table>
<thead>
<tr>
<th>Impact</th>
<th>2016</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of revenue or profit</td>
<td>54%</td>
<td>56%</td>
</tr>
<tr>
<td>Loss of customer confidence</td>
<td>33%</td>
<td>32%</td>
</tr>
<tr>
<td>Reputational damage</td>
<td>33%</td>
<td>35%</td>
</tr>
<tr>
<td>Loss of supplier confidence</td>
<td>9%</td>
<td>17%</td>
</tr>
<tr>
<td>Loss of employees</td>
<td>6%</td>
<td>8%</td>
</tr>
<tr>
<td>Loss of market share</td>
<td>3%</td>
<td>4%</td>
</tr>
</tbody>
</table>

**If you have suffered an attack in the past year, what was the impact on the business?**

Given the possible punitive penalties instilled by regulations, such as GDPR, for negligence, it is unsurprising that data loss incidents are by far the most feared form of security breach. Almost three-quarters of respondents (72 per cent) are concerned by them.

### Data loss is causing the most concern

<table>
<thead>
<tr>
<th>Incident</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data loss incident</td>
<td>39%</td>
</tr>
<tr>
<td>Phishing / social engineering</td>
<td>26%</td>
</tr>
<tr>
<td>Service interruption</td>
<td>19%</td>
</tr>
<tr>
<td>Virus / malware outbreak</td>
<td>12%</td>
</tr>
<tr>
<td>DOS / DDoS</td>
<td>4%</td>
</tr>
</tbody>
</table>

**Thinking about the next two years, which two threats are you most concerned about?**

While 45% of respondents are concerned by data loss incidents, respondents (72 per cent) are concerned by them. Almost three-quarters of breaches is a loss of supplier confidence with almost double the amount of respondents citing it as an effect compared with 2016.

### Just over half of respondents have fully identified assets that need protecting (55%)

Just over half of all respondents (55 per cent) consider that they have fully identified the assets within their organisation that need protecting. A further 38 per cent are still on the identification journey.

**VULNERABILITIES**

Just over half (54%) of all respondents have systems in place to fully identify security vulnerabilities. Almost one in ten (9 per cent) either have no such system or are unaware of them.

Our research shows that less than a third (32 per cent) of all respondents have systems in place to fully identify security vulnerabilities. Almost one in ten (9 per cent) either have no such system or are unaware of them.

Almost one in ten have no system in place to identify new security vulnerabilities.

**Have you identified which assets need most protection in your organisation?**

Our research shows that less than a third (32 per cent) of all respondents have systems in place to fully identify security vulnerabilities. Almost one in ten (9 per cent) either have no such system or are unaware of them.

**Do you have systems in place to identify new security vulnerabilities in your technology?**

Vulnerability management is hard. It’s the constant race against exploits in known holes in your software and getting these patched. It’s not impossible though; IT and Security need to work together to ensure vulnerabilities are disclosed and prioritised. It’s worrying to see that almost two-thirds of respondents don’t have a mechanism for identifying vulnerabilities. Identification is only part of the solution – a clear process to remediate is also key.

**Christian Toon, CISO, PwC**
Move towards more proactive approach to cyber security

Overall, how would you describe your organisation’s approach to cyber security?

Almost two in ten lack processes to fix vulnerabilities in a timely manner

While an encouraging 80 per cent of respondents feel that they have the correct processes in place to fix vulnerabilities in a timely manner, almost two in ten (18 per cent) do not.

Do you have a process in place to fix vulnerabilities in a timely manner?

REGULATORY COMPLIANCE

GDPR has focused organisations on their security compliance obligations over the last 12 months. This has been evidenced by much people-focused activity within industries including hiring and use of consultants. It remains to be seen whether this step up in activity will be maintained over time, or if organisations will feel that they have ticked a GDPR box for the moment. Cyber security professionals will play an important role to ensure compliance is maintained long term, and if organisations have made the necessary link through to the need for early detection and timely response then activity around regulatory compliance should remain at an increased rate.

In 2018, 60 per cent of our research respondents state that the regulatory bodies that govern their organisations do not provide useful guidance on how to mitigate cyber security risks. This has increased from 54 per cent in 2016.

Respondents feel less guided by regulatory bodies

Do you feel the regulatory bodies that govern your organisation provide useful guidance to help you manage your cyber security risk?
In addition to ISO 27001, one scheme that many companies are increasingly benefiting from is the Cyber Essentials scheme, a UK government-backed security standard that identifies the security controls an organisation must have in place within their IT systems. Our research shows that usage of this standard has increased by 61 per cent since 2016, which is great news.

Growing use of Cyber Essentials as regulatory compliance standard

<table>
<thead>
<tr>
<th>Standard</th>
<th>2015 Percentage</th>
<th>2018 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>82%</td>
<td>61%</td>
</tr>
<tr>
<td>Cyber Essentials</td>
<td>34%</td>
<td>56%</td>
</tr>
<tr>
<td>NIST</td>
<td>48%</td>
<td></td>
</tr>
<tr>
<td>PCI DSS</td>
<td></td>
<td>53%</td>
</tr>
<tr>
<td>HMG</td>
<td>22%</td>
<td>21%</td>
</tr>
</tbody>
</table>

Does your organisation use any regulatory compliance standard to mitigate cyber risk?

While Europe’s attention has been heavily focused on GDPR, there are other regulations that CISOs and cyber security professionals must manage. Most notably is the Networks and Information Systems (NIS) Directive, which aims to improve the EU’s preparedness for cyber attacks, particularly on critical infrastructure such as energy, utilities, finance, healthcare, digital infrastructure and transport. This regulation means that cyber professionals operating in these industries and the public sector will have to implement high defences against cyber attacks.

Almost two-thirds of organisations have appointed a dedicated DPO

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>65%</td>
</tr>
<tr>
<td>No, but another role is covering this</td>
<td>35%</td>
</tr>
<tr>
<td>No, and no other role is covering this</td>
<td></td>
</tr>
</tbody>
</table>

Does your current organisation have a dedicated Data Protection Officer?

Convincing organisations that data protection is a source of competitive advantage and not a cost centre could be effective at driving greater compliance. Consumers remain doubtful about the ability of merchants and service providers to protect their personal data, in no small part due to the bad press surrounding data breaches and misuse at Facebook, Yahoo and Uber amongst others. The role of a Data Protection Officer is key but revolves around the objective to ensure consumers’ data privacy is maintained, and personal data is protected from misuse. Sixty-three per cent of respondents have a DPO in a dedicated role and a further 31 per cent have another person covering this role.

SECURITY SKILLS

The search for senior cyber leadership has tailed off dramatically with only 14 per cent of respondents indicating a skill gap this year compared with 38 per cent in 2016. The search for security operations professionals tops the requirements list with more than half (52 per cent) of respondents citing a need for more, which is interesting given the increase in outsourcing of security operations. Architects and penetration testers are also less sought after than in previous years.

Leadership in place but operations posts need to be filled

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security operations</td>
<td>52%</td>
</tr>
<tr>
<td>Security training and awareness</td>
<td>43%</td>
</tr>
<tr>
<td>Security architecture</td>
<td>42%</td>
</tr>
<tr>
<td>GDPR / data protection</td>
<td>38%</td>
</tr>
<tr>
<td>Security engineering</td>
<td>30%</td>
</tr>
<tr>
<td>Governance, risk and compliance</td>
<td>30%</td>
</tr>
<tr>
<td>Security project management</td>
<td>26%</td>
</tr>
<tr>
<td>Senior cyber leadership</td>
<td>21%</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>14%</td>
</tr>
<tr>
<td>Cyber leadership</td>
<td>12%</td>
</tr>
</tbody>
</table>

If you have indicated you are lacking ‘internal cyber skills’, what skills do you feel you are lacking?
The cyber security skills arena has matured considerably since our last survey and experience is becoming as important as accreditation. While this could also be driven in part by skills shortages, just over a quarter (27 per cent) of respondents care little about accreditation, preferring to make hiring decisions based on previous roles and experience.

Experience increasingly more important than accreditation

| Not - accreditations matter very little, only experience matters | 14% |
| Quite – it’s a contributory factor, although we sometimes hire without it | 52% |
| Very – it’s a key factor, we would rarely hire without it | 30% |

When hiring people, how important is it for them to have some kind of accreditation?

What accreditation do you value most?

- CISSP
- CCSP
- CGS
- GIAC
- SANS
- ISACA
- SABSA
- TOGAF
- CISM
- CRISC
- OSCP
- ITIL
- CREST
- CRISC
- ISO27001
- ISC2
- EXPERIENCE
- ISO2001

ALL ABOUT HARVEY NASH AND INVINSEC

Harvey Nash

Our Information Security Practice is our specialist team that is solely dedicated to this increasingly business-critical function. Over the past five years the team has seen over 10 per cent year-on-year increase in demand for security-related skill sets across the UK alone. This is a clear response to the ever-changing threat landscape and the challenges all organisations face in keeping data and assets secure. Our extensive global network and talent pool mean our team can provide bespoke resourcing strategies to meet this demand. Our Information Security Practice offers a complete end-to-end recruitment service. We deliver permanent, contract and statement of work resourcing solutions across technical cyber, governance, risk and strategic security transformation skill sets. We have a successful track record of placing professionals at Global Chief Information Security Officer level through to entry-level Security Analysts. Our team is also heavily involved in thought leadership and advisory services, and has contributed to articles in Computing magazine and publications by Bloomberg.

James Walsh
Head of Security Practice

E: james.walsh@harveynash.com
T: 0121 717 1946
M: 07896 019475

Invinsec

Invinsec is a hyper-growth, British-owned cyber security company that specialises in security monitoring (SOC/SIEM). Headquartered in Cheltenham and with offices in Birmingham, it aims to be the number one company in the UK and Europe for security monitoring by 2021.

Founded in 2016, it is ripping up the rule book for security monitoring with tech you can use quickly at prices you can afford, and with first-class service too. Invinsec built and owns its cloud-based software platforms BroadBot and StopPoint, and has its own 24/7/365 SOC service with UK SOC locations in Cheltenham and Birmingham.

Invinsec is staffed by veterans of the military, law enforcement and secure government agencies. It provides state-of-the-art security monitoring to businesses of all sizes – at a price they can understand and afford.

A Great British company providing security monitoring for everyone.