Savannah®
THINKING BEYOND

savannah-group.com

Cybersecurity
Is your Board on board?

SAVANNAH WHITE PAPER

Over the last 12 months, Savannah has been inundated with requests from boards for help in providing CISO expertise.

To better understand this growing market, Savannah surveyed 36 top CIOs about what cybersecurity looks like in their organisation and how effective they see it to be in protecting against cyber threats.

Our research has shown that the most important criterion for an organisation to feel well protected is not the size of budget allocated to security or the specific technical platform, but good governance and oversight.

- Budget doesn't increase confidence
- Board buy-in is key to making a CIO feel confident about security
- This, we found, can be achieved by good governance

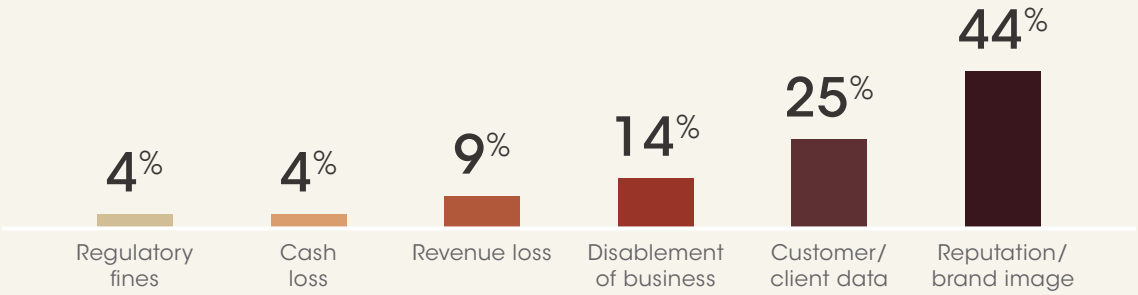
The cost of a data breach can be disastrous for any organisation. In 2015, we saw TalkTalk breached for the second (but possibly third) time within a year, compromising 157,000 personal records and costing the company an estimated £60m as well as the loss of over 100,000 customers (itpro). However, the irreparable damage done to the company's brand and the steady flow of customers still jumping ship—126,000 customers switching away from the provider in the first three months of this year (theregister)—leaves the organisation in a difficult position.

The most high profile hack of 2015 was of course the 'meetup' website, Ashley Madison, from which 30m users' information was stolen and then published online. The hack could cost parent company, Avid Life Media, £1.2bn in the UK alone according to the law firm, Pinsent Masons, while the company already faces a $576m class-action lawsuit in the US. Along with a huge dent to its finances, the hack has delivered irreparable reputational damage.

Other notable attacks of the year include one of the US's largest health insurance providers, Anthem, which lost nearly 80m records, while Target settled $39m after a data breach affecting several US banks and 40m customer records.

The rise of ransomware and the possibility of malware moving from end-point targets into the cloud as well as the Internet of Things (IoT) introducing a whole new frontier of vulnerabilities, makes 2016 and beyond a volatile prospect for companies of any sector.

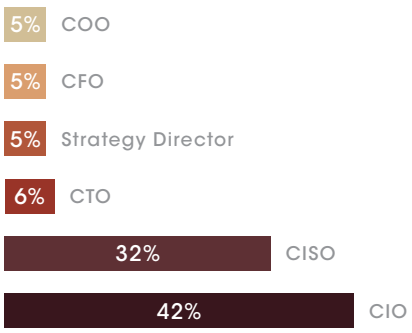
SHOULD THERE BE A BREACH, WHAT WOULD BE THE MOST WORRYING?



The threat landscape is evolving rapidly and security professionals continue to face new and developing threats. In 2015 over 500m on personal records were lost (Symantec) and this trend continues to increase year on year. According to a recent Ponemon Institute study, the average cost of a data breach is $3.79m.

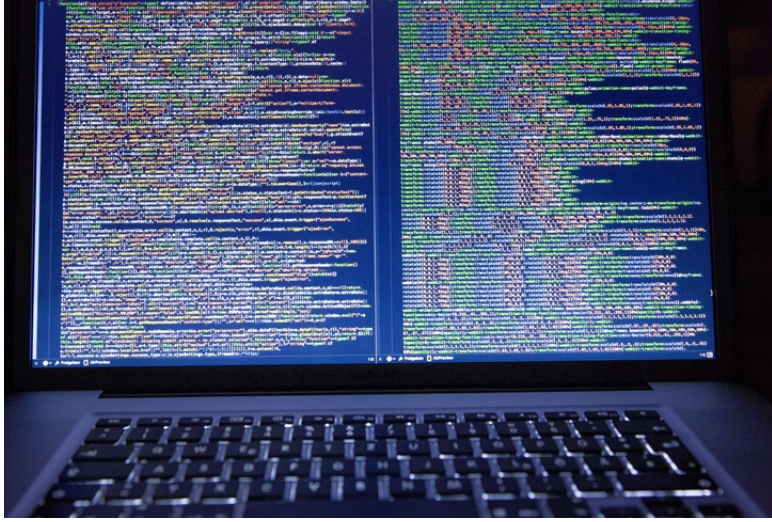
This alarmingly high figure only looks set to escalate, partly due to the impending implementation of the new GDPR regulations coming into effect in early 2018, which will mean fines of £20m or 4% of global turnover for breaching data protection regulations. Consequently, more than ever before, it becomes imperative that organisations have flawless security procedures. These alarming statistics mean that boards are now having to take cybersecurity extremely seriously.

Does your CEO/Board member hold a C-level executive accountable for cyber security management? If yes, what is their title?



The resignation of Target's CEO and CIO following the aforementioned breach shows that responsibility for the loss of data no longer solely rests on the CISO and it is therefore imperative that the CEO and CIO are well informed about the current security threats to their business. In a recent Ponemon Institute study, 79% of C-level US and UK executives surveyed say executive level involvement is necessary to achieving an effective incident response to a data breach and 70% believe board level oversight is critical.

Our research shows that within the majority of organisations, it is the CIO or the CISO who has accountability for cybersecurity management, however, a recent Veracode study found that when a breach occurs it is the CEO that the board holds accountable. As accountability is at the highest level, security is now fundamentally integral to any organisation.



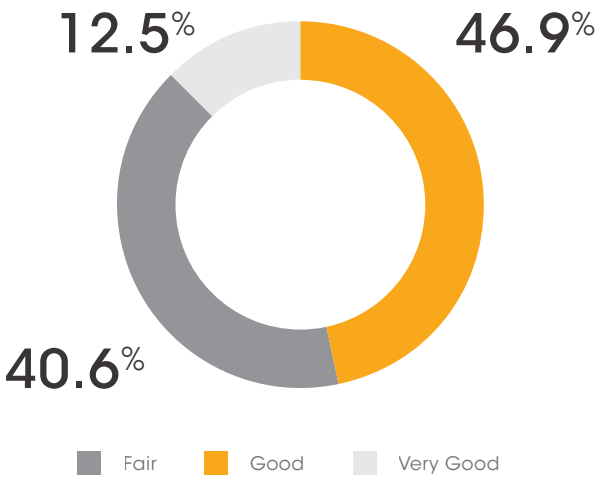
CIOs remain uncertain about their companies' ability to protect themselves from cyber threats.

Of the 36 CIOs we surveyed, nearly 40% said they did not have sufficient budget to implement the organisation's security programme. However, there was no significant increase in how well protected the CIO feels the organisation is when the budget is seen to be sufficient.

No respondent would class their company as excellently protected, while only 12.5% would say that their protection from cyber threats was very good. Alarmingly, 40.6% of those surveyed would only class their protection as fair.

We wanted to explore how communication and good governance within an organisation affects the board's and CEO's understanding of the evolving threat landscape. We investigated whether a cybersecurity senior management committee or regular review of the organisation's cybersecurity framework implementation plan had an impact.

How well protected do you feel your organisation is from cyber threats?

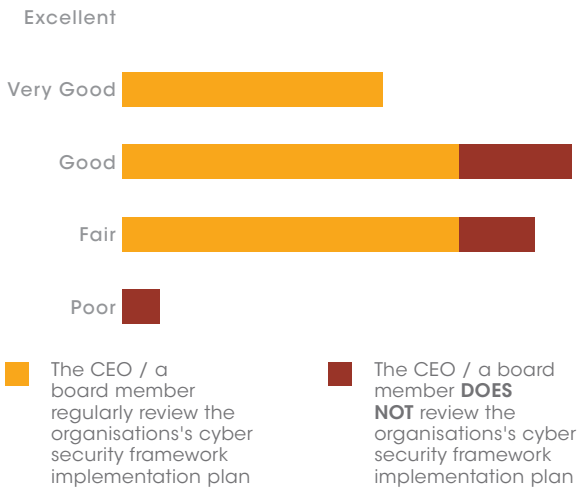


Regular reviews of the cybersecurity framework implementation plan

More than 90% of corporate executives said they cannot understand a cybersecurity report and are not prepared to handle a major attack, according to a new NASDAQ commissioned survey.

However, we found only when a board member regularly reviews the organisation's cybersecurity framework can the CEO's understanding of cybersecurity be classed as very good (22%). Therefore, it is imperative that cybersecurity matters are discussed at the board table and that someone at board level has security within their remit.

How would you grade your CEO's understanding of information and cyber security?



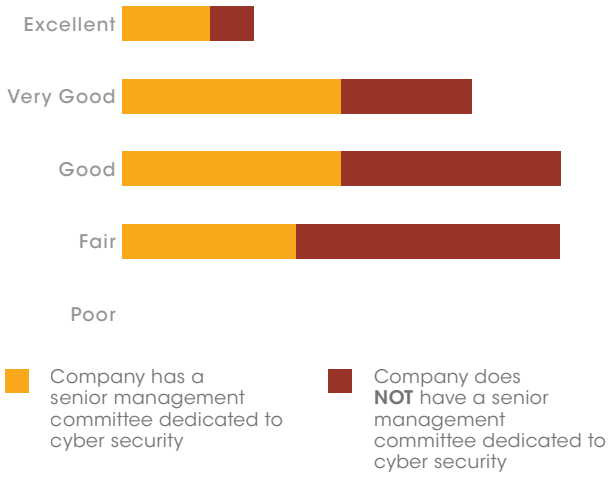
Cybersecurity management committee

Those companies with dedicated security management committees are better at keeping their boards educated about current threats. 67% of boards 'excellently' apprised of current threats had a cybersecurity management committee compared to just 32% without.

It goes without saying that the more exposure the board has to security related issues the better informed they will be about the company's ability to deal with those threats.

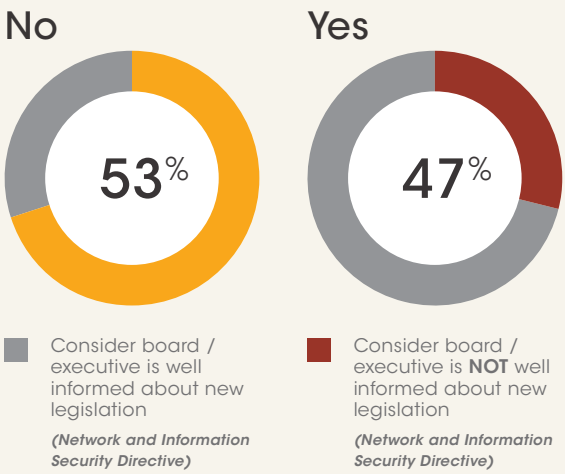
Of CIOs that felt the board/CEO had a very good understanding of current cyber threats, over 60% had a management committee dedicated to cybersecurity. Of those respondents that said their stakeholders had very good alignment in terms of threats, 75% had a cybersecurity dedicated management committee.

How well do you think your CEO / a board member stays apprised of current cyber threats relevant to your organisation?



We can see how a dedicated cybersecurity management committee impacts how well informed the board is about current and upcoming legislation. Of the 53% without a management committee, only 30% said their board is well informed of legislation, compared to over 70% when there is a management committee in place.

DOES YOUR COMPANY HAVE A SENIOR MANAGEMENT COMMITTEE DEDICATED TO CYBER SECURITY?



Take away points

As cybersecurity becomes one of the key business risks for companies, boards are taking a keen interest in the topic.

Good governance is the most important criterion for an organisation to feel well protected and, arguably, better prepared for a breach—more than allocated budget or technical platform.

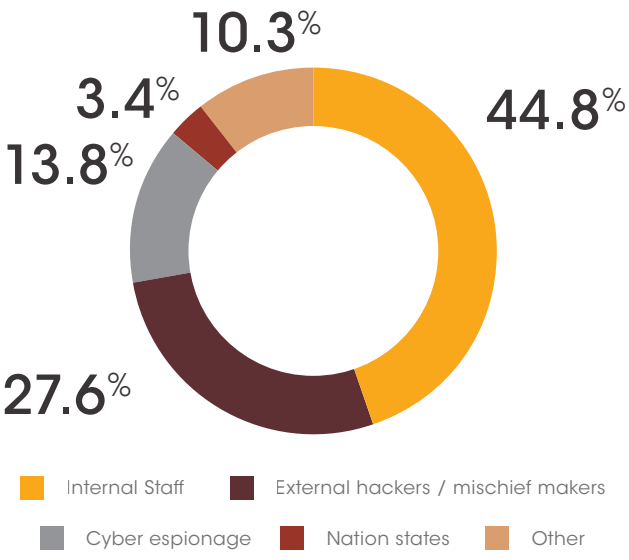
The CEO and CIO are held accountable by the board and thus need a highly capable and competent cybersecurity expert in place.

It is vital that a CISO can engage with the board to ensure its understanding of the issues involved.

Today's CISO needs to combine technical strength and the ability to "think like a criminal" with the outstanding stakeholder management and leadership skills to interact at board level. Individuals who possess all these skills are rare and expensive but they do exist.

The question is, how will you attract the very best talent to your organisation?

From where do the greatest threats to your organisation come?



In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches and cyber-attacks. However, there is a growing concern about the potential damage to reputation, class action lawsuits and costly downtime and this is motivating executives to pay greater attention to the security practices of their organisations.

Report prepared by:

Philippa Mack and James Davis

Vicky Maxwell

Partner | Digital & Technology Leaders Practice

vmaxwell@savannah-group.com

+44 (0)20 3781 7486

James Davies

Researcher | Digital & Technology Leaders Practice

jdavies@savannah-group.com

Philippa Mack

Research Consultant | Digital & Technology Leaders Practice

pmack@savannah-group.com

About Savannah

Savannah combines the quality, agility and personal attention of a boutique search and interim firm, with the resources and global capability of a larger firm.

Our innovative global structure, agile service delivery and integrated search and interim practices, gives you access to people that simply aren't accessible to other firms. It's the reason why more than 600 of the world's leading brands have chosen to use us, and why 85% of our revenue is from repeat business.

For more information on Savannah's cyber security practice which helps organisations find permanent or interim CISOs, please contact its leader Vicky Maxwell Davies **vmaxwell@savannah-group.com** on **+44 (0)20 3781 7486**.

Executive Search | Interim Management | Executive Assessment & Development | Market Intelligence

Savannah
THINKING BEYOND

www.savannah-group.com