Bitdefender

Small Gains, Big Wins

2018

A study on the pressures infosec executives face, and their attitudes towards cybersecurity risk

Bitdefender

Foreword

"I guess it's not surprising that it's taken another confidence-busting incident like WannaCry to begin turning the crank on organisational cyber maturity improvement — but in security it is usually only when something goes fundamentally wrong that business leaders realise something needs to change. As a CISO myself, I'm really starting to see greater improvements in our reporting lines, all the way to the board, and our jobs are far better defined. I think over the next couple of years we'll continue to see organisations dramatically improving their overall security posture — the risk of doing nothing is just too great.

"UK CISOs are, by large, in a much improved position. Overall risk awareness is up, strategies are being improved and corporate infosec budgets are slightly more flexible than they have traditionally been. Complacency among information security professionals seems to be falling at the wayside, and the large-scale security incidents of the last 12 months have certainly paved the way for a new raft of infosec policy changes throughout UK businesses."

Marc Lueck, CISO at Company85

Introduction

Introducing Bitdefender Small Gains, Big Wins - a comprehensive study of the cyber security attitudes of UK CISOs, CSOs and CIOs

On a trading floor, a millisecond can mean losing thousands. The stakes are even higher in information security, where small differences, seemingly imperceptible for some, can actually mean the difference between an organisation succumbing to a breach or completely safeguarding itself.

Business leaders are starting to realise the complex threatscape that now exists in 2018, and the associated repercussions should a data breach occur. It is therefore now quite common for larger organisations to have a dedicated CISO or CSO, either reporting in directly to the CIO, or the wider C-suite. This triumvirate of job roles is tasked with keeping organisations safe and secure — however that end goal is not without its challenges.

The good news? Very often, an organisation's information security profile can be boosted exponentially without significant investment. By implementing small swift changes to training routines or through lightweight, quick to implement infosec tools, potential entry points for cyber criminals can be closed and associated risks reduced. Through these simple changes of infosec strategy, long term gains in confidence aren't far away.

This focus on small changes, and the associated big infosec wins, has led us to conduct this study — focusing around the following three themes:

- Risk - exploring how C-level security executives view the current external threatscape, and how this influences internal risk
- Speed - identifying where within the security stack that speed of execution and swift decision making is the most vital
- Strategy - hearing directly about current and future infosec strategies from CISOs and CSOs on the front line, and seeing what changes have had the biggest impact

The study shows that many infosec executives have been stung by recent global threats such as WannaCry, which has in turn dented confidence and caused them to take a hard look at existing organisational policy. The biggest threats lie in data-heavy departments, and with managers who are all too laissez-faire in their attitudes to cyber security. To combat this, infosec executives are bringing training to the boardroom and beyond, and many are implementing cloud-based data protection tools to stay one step ahead. One thing is for sure, CISO and CSO roles are becoming far more strategic, and all the more integral to ensuring the success of businesses into 2018 and beyond.

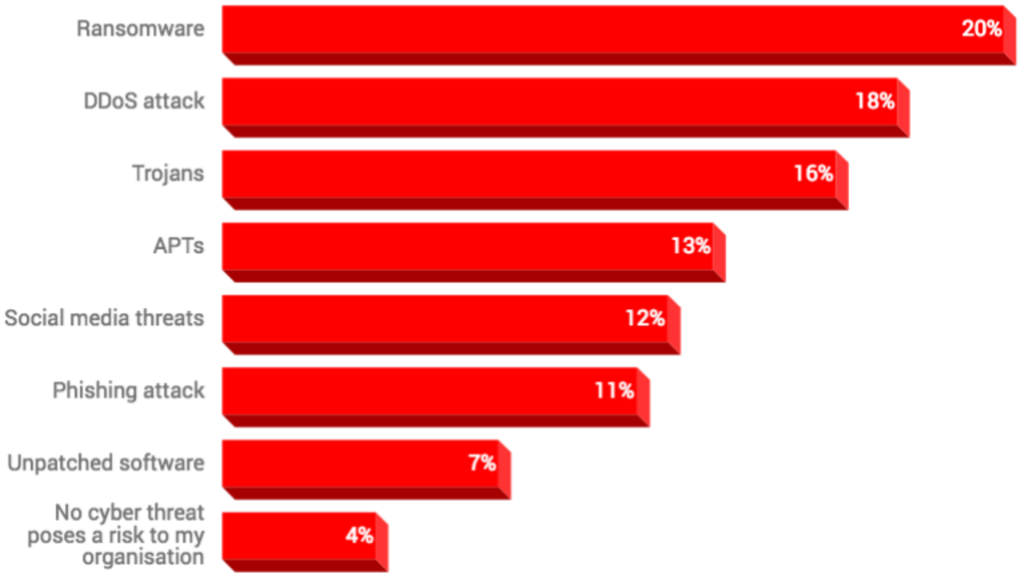
Bogdan Botezatu, Senior Cybersecurity Analyst at Bitdefender

Assessing the Threatscape: Risk

Understanding how CISOs, CIOs and CSOs perceive the current cybersecurity threat landscape and the risks to their organisations, is key in highlighting areas for security improvement.

Its been a landmark 12 months for high-profile cyber breaches, but which attack vectors are feared the most by organisations in 2018?

Infosec executives believe the following cyber risks / threats pose the biggest risk to their organisations:



Following on, from the now infamous WannaCry and GoldenEye / NotPetya attacks in 2017, ransomware is today perceived as the top cyber threat. In fact, one in five (20%) of infosec executives cite it as their biggest external risk.

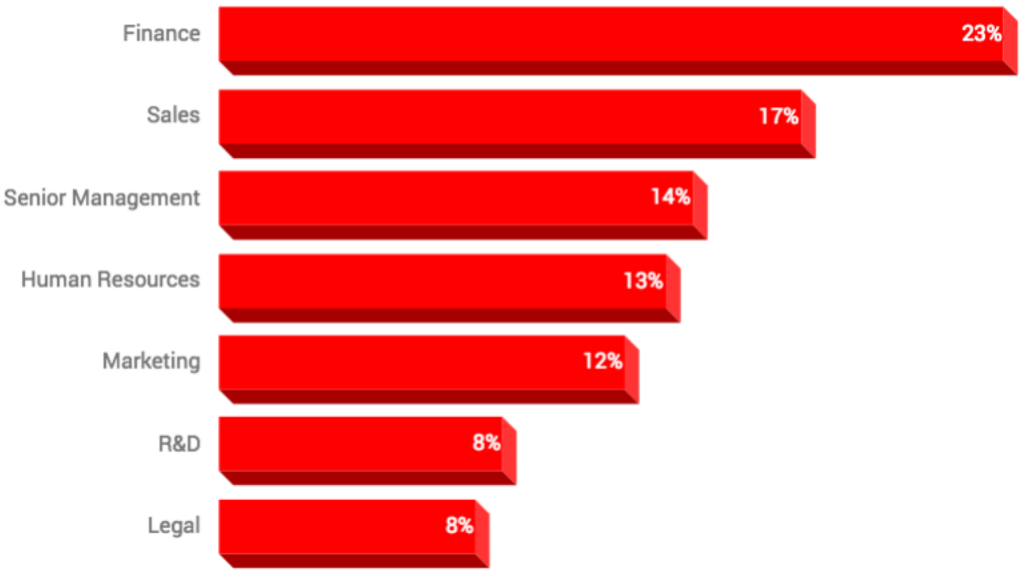
DDoS and trojans follow in second and third place, taking 18% and 16% of the vote respectively, likely due to their ability to inflict extensive damage to corporate systems with little or no notice.

Different roles, different risks

CISOs are most concerned about the threat of trojans (22%), while CIOs perceive the most risk lies with ransomware (33%).

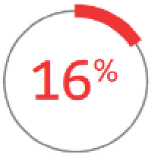
Are all organisational departments created equal when it comes to the risk of being hit by a data breach?

Infosec executives believe the following organisational departments are most at risk of a data breach:

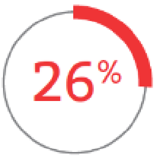


Departments which infosec executives deem to be most at risk, all handle large amounts of sensitive information — which could be potentially lucrative if sold on by bad actors. Finance and sales tops the list, with 23% and 17% respectively, followed closely by senior management with 14%, and HR with 13% of the vote.

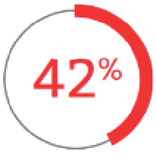
The effects of succumbing to a data breach are wide ranging, but what are infosec executives most concerned about when it comes to repercussions?



Loss of employee trust



Fined by regulatory authority



Loss of customer trust

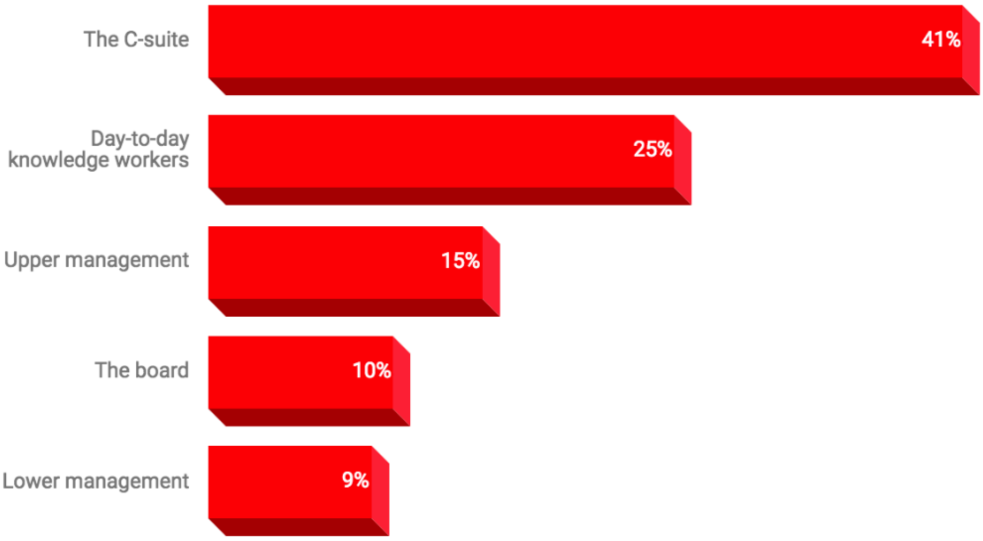
Aside from learning how it happened and putting safeguards in place to ensure it doesn't happen again, there are very few positive consequences of a data breach. At 42%, the major concern of infosec executives post-breach is a loss of customer trust, which would likely also cause knock-on reputational and financial damage.

Different age, different priorities

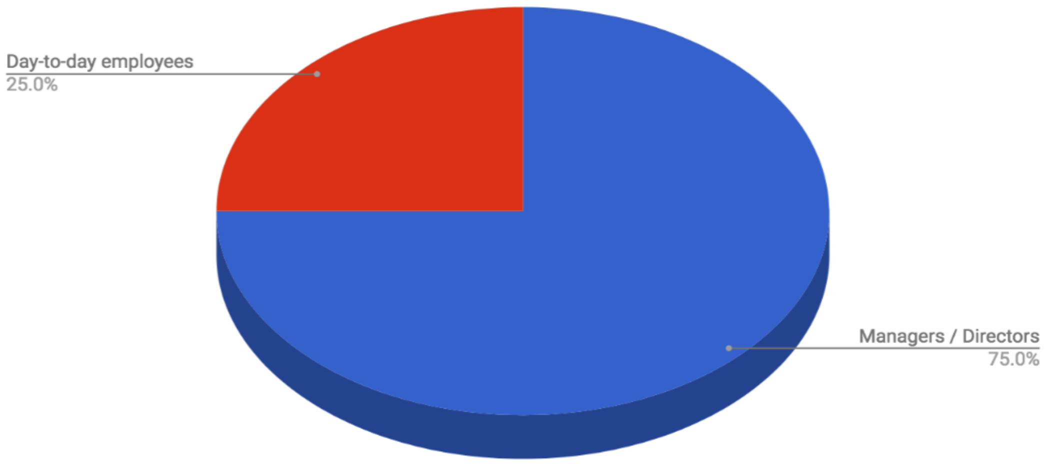
Older information security executives are more concerned about losing customer trust (73%), as whether younger infosec executives are more worried about being hit with a fine from a supervisory authority (29%), should a breach occur.

Not all is as it seems at the top of the organisation, and management might need to take a long hard look in the mirror...

Infosec executives believe the following organisational demographics are most likely to maintain poor infosec practices and not follow the rules laid out by the IT department:



Condensing down management levels (both senior and junior) and correlating this with day-to-day knowledge workers means that at least three quarters (75%) of infosec executives believe that managers are more likely to bend or break information security rules.



Clearly damage from flaunting the rules can extend beyond the walls of the organisation. However, is it any surprise given the circumstances?

52% of infosec executives think a recent breach had a negative effect on employee morale

58% of them have lost sleep worrying about a potential attack on their organisation

20% of them can't say for sure whether their company's endpoint security solution is up-to-date

Industry Insight

"A knee jerk response is no substitute for considered, measured action when it comes to cyber threats. This is why it's important for CISOs, CSOs and CIOs to surround themselves with a combination of the right infosec solutions, and a reliable security response team. However, in a world where there is an increasing infosec skills gap, this is easier said than done.

"The gap can certainly be narrowed in a couple of ways, the first is by placing more emphasis on the adequate training of staff, especially those in positions of management who need to set the right example to others within the organisation. The second is in regard to the gender divide which still exists within the technology space in the UK, specifically cyber security. Those infosecurity executives who are taking equality seriously in their recruitment processes are broadening their workforce with a demographic which approaches risk in a different way. Having a wider range of perspectives throughout an organisation, will stand it in far better stead for mitigating the multitude of threats which enterprises contend with in 2018."

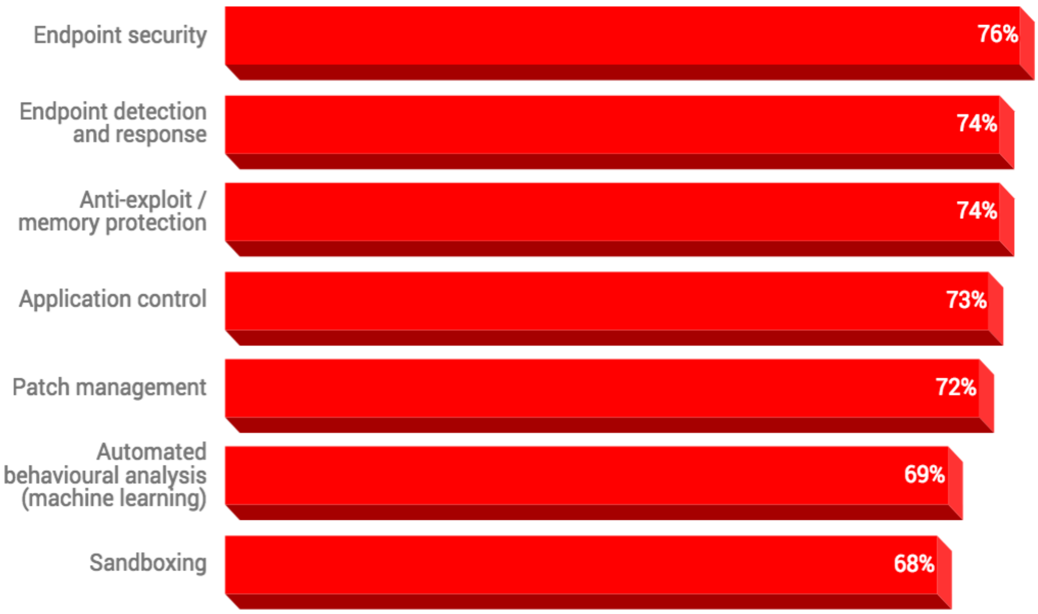
Jane Frankland, CISO advisor and author

Focusing attention inward: Speed

The speed at which organisations are able to identify and respond to threats — with a view on making small changes — can, if they are implemented correctly, immeasurably improve risk response.

Swift identification and mitigation against cyber threats could save an organisation from disaster, but in what areas of the security stack is speed most important?

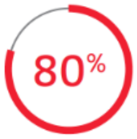
Infosec executives think that speed is either critically, or very important in the following areas of the security stack:



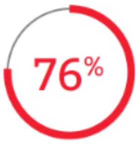
Endpoint security, detection and response are all areas in which speed is deemed most important by infosec executives, with 76% and 74% of the vote respectively. This is closely followed anti-exploit / memory protection and application control at 74% and 73%. As can be clearly seen in the above graph, speed is largely seen as a vital component across all the infosec solutions surveyed.

Infosec executives don't see the element of speed becoming any less important in regard to cyber security over the next decade...

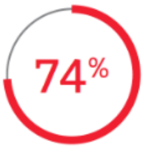
Infosec executives either agree or strongly agree with the following statements around speed in its relation to cyber security:



"Threat analytics, and the ability to quickly understand the data, is critical to both risk mitigation and business continuity in my organisation."



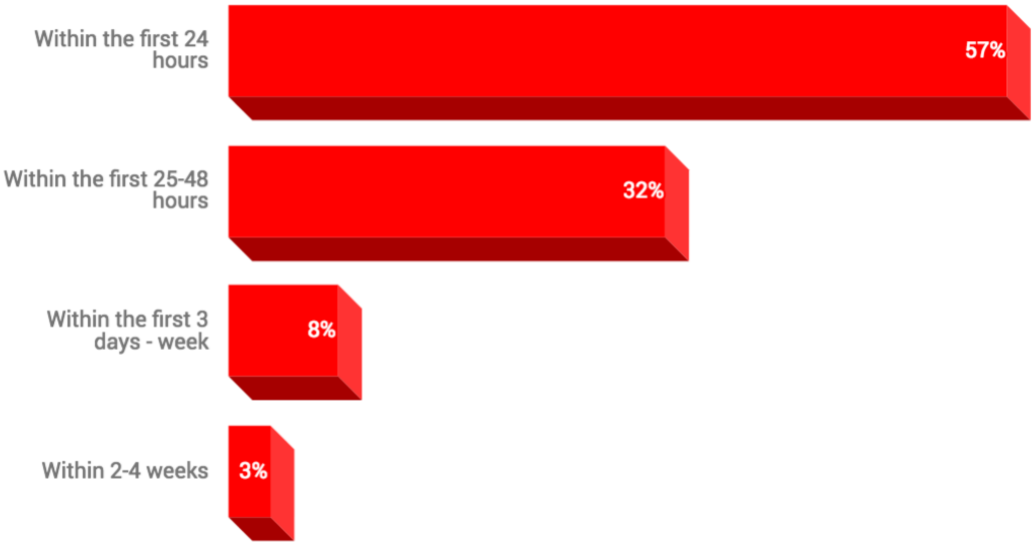
"Speed of infosec response will continue to be important over the next 10 years."



"Speed is an essential component of mitigating the damage around a cyber attack."

Global cyber threats such as WannaCry don't hang around once they are out in the wild. Just how quickly can organisations identify and assess global threats such as these?

Infosec executives believe that it would take the following amount of time before their organisation was aware of a new large-scale public cyber threat:



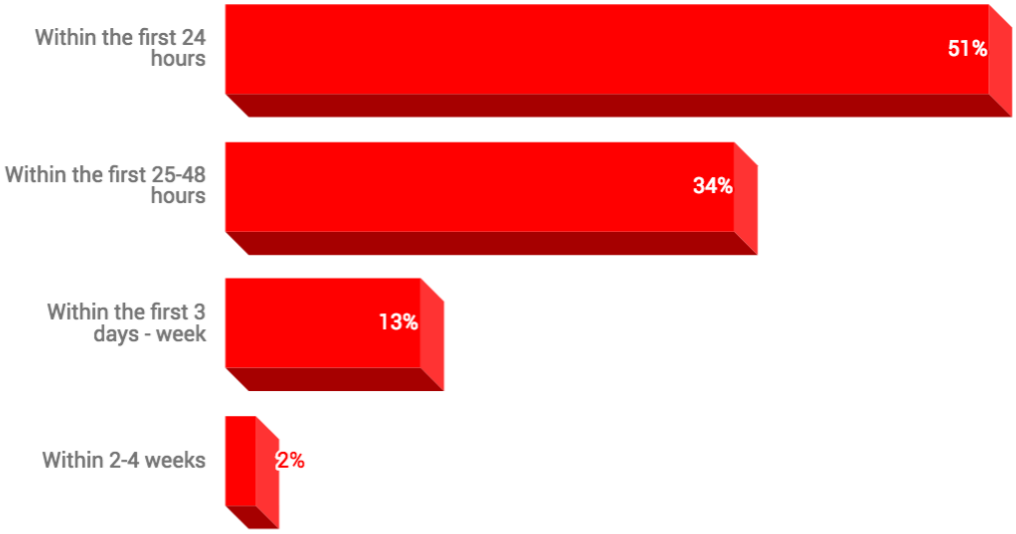
More than half (57%) of infosec executives will be aware of a large-scale public cyber threat within the first 24 hours of it being discovered, with a further 32% becoming aware within the first 25-48 hours. While this may seem like a reasonable reaction time, it is important not to underestimate the speed at which variants of modern malware can spread.

Bigger org. more aware

68% of infosec executives who work in organisations of 5,000+ employees will be aware of a large-scale cyber threat within the first 24 hours, compared to an average of 55% for organisations of 500 - 4,999 employees.

Awareness is one thing, but how about ensuring an organisation can be swiftly safeguarded against a global cyber threat?

Infosec executives believe that it would take the following amount of time to patch corporate devices (desktops, laptops and mobile phones) after discovering a vulnerability:



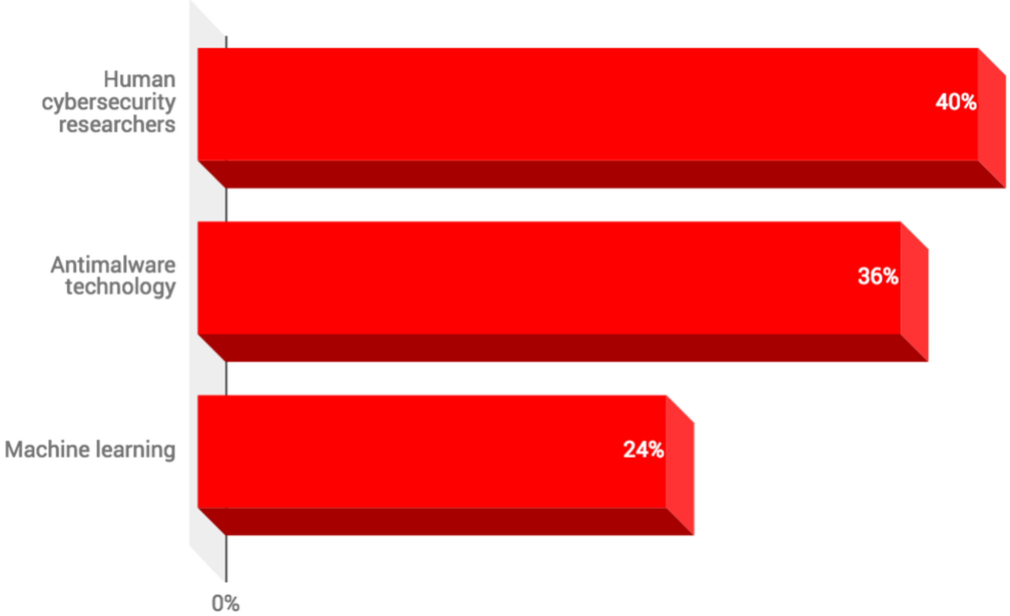
Just over half of infosec executives (51%) think their organisation would be able to patch against a global cyber threat within 24 hours, with 49% taking longer than this. Faced with modern malware variants such as WannaCry and NotPetya that can spread within hours, this is simply not quick enough.

Infosec executives seem to feel similar, with 77% of them agreeing or strongly agreeing with the following statement:

“Being able to quickly patch devices against any and all emerging vulnerabilities is vital.”

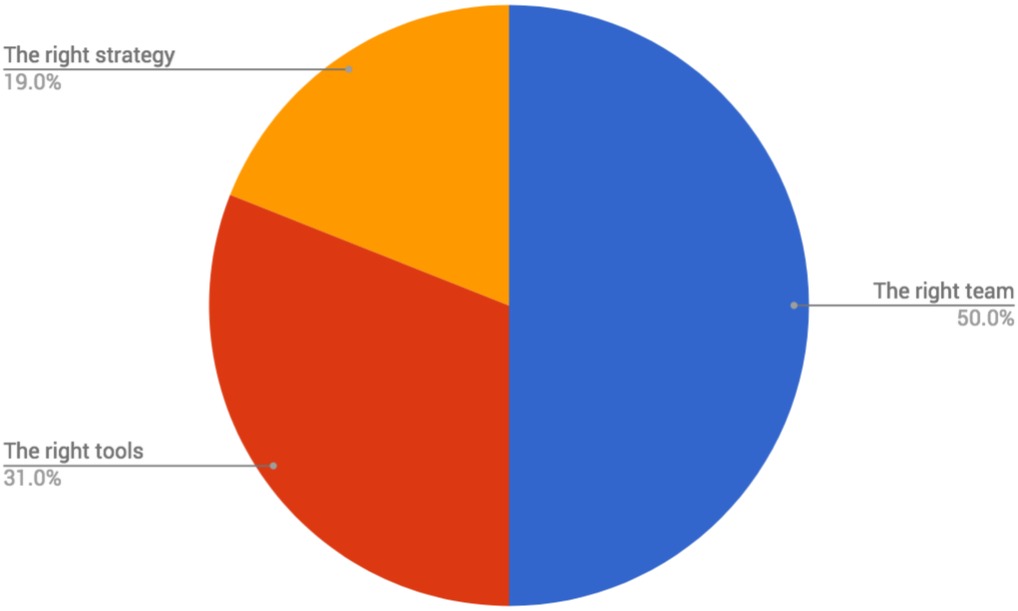
Threat detection and mitigation technology has developed exponentially in the last few years, but is it a worthy substitute for human intervention?

Infosec executives believe that the following factors are the most important when it comes to detecting cyber threats:



When it comes to detecting cyber threats human researchers are preferred by 40% of infosec executives, compared to antimalware technology (36%) or solutions utilising machine-learning (24%).

Infosec executives believe that the following factors are the most important in mitigating a data breach quickly:



Additionally, the focus on response and mitigation speed is very much centred around the human element, with 50% of infosec executives citing the right team is the most important. The right tools are seen as an important secondary factor with 31% of the vote, followed by the right strategy with 19%.

Different age, different strategies

When it comes to threat mitigation factors, older infosec executives are more inclined to angle towards strategy as being the most important factor in mitigating a breach quickly (36%), compared to younger execs (12%).

Small Gains, Big Wins: Strategy

Drawing insights which are actionable is one thing, but how these are implemented into a wider organisational security strategy is where the CISO, CSO and CIO will really prove their worth.

Being realistic when it comes to security strategy is the first step towards strengthening it. Are CISOs being honest or burying their heads in the sand?

Most infosec executives surveyed believe their organisation has suitable safeguards in place to protect against most modern day threats, however they also recognise that the threatscape is exponentially increasing — so understand that consistent auditing and accreditation is a must to encourage confidence across the organisation.

“Regular assessment and accreditation helps us understand the maturity level of our organisation, it acts as a standard for protecting our company against any cyber threat or attack.”

CISO of a banking corporation w/ 5000+ employees

Fortunately, none of the infosec executives surveyed believed their business was completely impenetrable to cyber criminals. After all, misplaced complacency can often lead to increased risk!

Human fallibility across the workforce is widely recognised as one of the biggest threats facing the enterprise, which is why infosec executives are placing greater emphasis on relevant training for employees which handle confidential corporate data.

“Infosec ‘awareness’ is one of our biggest weaknesses, and I’m trying to make higher authorities aware about this board meetings. I take regular meetings with various HODs (Head of Department) to make them more aware about basic steps which should be followed on daily basis.”

CISO of a financial entity w/ 1000+ employees

Additionally, suitable categorisation of sensitive data types is a must, to mitigate damage against a possible data leak. According to those surveyed, this is a key responsibility of the modern day CISO / CSO and certainly one they should be incorporating into their role.

Quick, easy to implement changes can have a surprisingly big impact on security strategy. But which of these are leading the charge amongst the infosec C-suite?

Nearly every infosec executive surveyed mentioned the smallest, but most effective change they’ve implemented has been to increase end-user awareness to the variety of different threats and attack vectors which are currently being exploited by cyber criminals. This can range from regular training programmes teaching employees what to look out for, right through to a more ‘shock tactics’ approach, where IT conducts mock-phishing and social engineering attacks on employees. While this might sound severe, you can guarantee it will stick in the mind of those affected.

“I would suggest that every organisation carries out more awareness programmes to keep every employee updated on the various cyber-attacks happening around the globe. This will help significantly to manage future ad-hoc threat situations.”

CISO of a telecoms company w/ 5000+ employees

Additionally, lots of infosec executives made positive reference to robust and easy to implement endpoint protection tools, often cloud-based (therefore continuously updated with the latest threat data) in order to mitigate the threat of new and emerging malware variants. Also, the best-in-class solutions on the market today should easily be able to provide protection against new software exploits, until IT admins can catch-up and patch affected software.

A common consensus

“Sometimes the smallest infosec changes can have the biggest impact on overall cyber security health.” A significant 71% of infosec executives agree with this statement.

The cyber security domain certainly isn’t standing still, and fortunately, neither are infosec pros. How will their roles develop in the future and what are they building out in the next 12 months?

The roles of the CISO and CSO will continue to grow in importance over the coming years. Initially largely just tasked with little more than implementing infosec tools, their positions in 2018 have well and truly evolved. Consulting the board on fundamental business and process changes to reduce risk, conducting company-wide training and awareness programmes, not to mention being on the frontline in regards to regulatory compliance, such as the GDPR.

“Presently, security is in the limelight and organisations are investing to build out their infosec capabilities. Today, CISOs are considered an integral part of board meetings, and their suggestions are considered very important when it comes to budget allocation. The modern-day CISO now requires both business knowledge as well as technical capability, for better communication between IT teams and senior management.”

CSO of an information security company w/ 1000+ employees

Infosec executives are now spending more time focusing on how to speed up patching software against new vulnerabilities. In addition, more tools are being built out to identify anomalous movement or transfer of data on endpoint devices — aimed at stopping malware before it can become a company-wide issue.

Looking further ahead, infosec executives are focused on technologies such as artificial intelligence and machine learning, and how these can be successfully leveraged to build out a company’s cyber security profile.

“Moving towards automation and making changes in the organisation to achieve further digitalisation will help us match the pace of technology, and will give our IT specialists the upper hand when it comes to new cyber threats.”

CISO at an insurance firm w/ 5000+ employees

Conclusion

Many infosec executives are losing sleep at night about information security threats, but their direct C-Suite colleagues are the biggest culprits when it comes to flaunting the rules. The CISO, CSO and CIO need to be tougher at conveying the real life repercussions of poor information security practices, from the board level downwards.

Incremental speed gains across the security stack are important, as when added up can make a profound difference at detecting and mitigating threats. Consider whether your endpoint security, detection and response solutions would currently be efficient enough in dealing with a new ransomware variant, for example. Speed of response will continue to be vitally important throughout next decade and beyond.

Information security is an ever-evolving and changing process, with advancements in technology not only increasing the threat landscape, but also the protective tools available — a double-edged sword for infosec executives. Being able to accurately categorise and monitor sensitive information in real-time is also seen as a key requirement in mitigating the damage around a breach.

The time to awareness for emerging information security threats is relatively good, but there is still room for improvement. This also rings true when it comes to patching and updating devices against emerging threats, and is where a continually updatable cloud-based security architecture can help, such as that which Bitdefender’s GravityZone product suite is built upon.

Automated threat intelligence is important, and many infosec executives are embracing technologies such as machine learning within their security stacks, but its not yet a substitute for real human information security researchers. For the foreseeable future, having the right security response team around you is key for effectively mitigating threats.

Both CISO and CSO roles are continuing to evolve. People in these positions are now far more likely to have a seat at the boardroom table due to recent global attacks thrusting cybersecurity into the limelight. Moving forward they will start to be responsible for fundamental business and process changes to reduce risk.

About Small Gains, Big Wins

The Bitdefender Small Gains, Big Wins Study explores, in detail, the pressures faced by CISOs, Chief Security Officers (CSOs) and Chief Information Officers (CIOs) and their attitudes to risk, speed and strategy when it comes to information security. Research was conducted by Censuswide on behalf of Bitdefender amongst 250 CIOs/CISOs/CSOs, who have control over IT budgets and influence/make security decisions, in UK-based companies with 500+ employees. The qualitative element of the research, also conducted by Censuswide, mapped the long-form opinions of four CISOs and one CSO across four industry verticals.

About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on.

Contact Us

www.bitdefender.co.uk

01344 709 113

publicrelations@bitdefender.com

twitter.com/Bitdefender_Ent

FOR MORE INFORMATION VISIT: bitdefender.com/business