Winning the Cyberwar

Enabling UK Business Now and in the Future
Contents

Foreword: The New Era of Cyber Attacks .................................................. 3
The Invisible Challenge ............................................................................. 4
The Unrelenting Cost ............................................................................... 6
Business Must be the Driver of Change .................................................... 8
Arming your Business with Confidence for Today and Tomorrow .......... 10
Foreword:
The New Era of Cyber Attacks

Cyber attacks are entering a new era. Increasingly sophisticated attacks, such as the hacking of a multi-billion dollar entertainment company and the takeover of a government social media platform, suggest that any institution (public or private) can be targeted. These events reflect how cyber attacks present a growing threat for companies, and contribute to unprecedented reputational and financial damage to businesses. Figures suggest that the cost of cyber attacks to the UK is £27bn per annum\(^1\), posing a huge worry to UK businesses, particularly those storing large amounts of confidential or sensitive data.

The stakes are therefore high for companies lacking the necessary security resources, and even higher for those ambivalent or unreactive to information protection issues.

Our research, based on an online survey of 505 UK IT decision makers, provides a snapshot of how those individuals feel about the state of their corporate security strategy today - their data security defences, culture and priorities. To a large extent, it reveals that despite the growing data security anxiety, many UK companies currently lack both the confidence and expertise to effectively tackle cyber attacks. This puts many companies at risk of suffering from the financial and reputational consequences.

Left unchecked, this problem is only set to get worse. In order to tackle the highly sophisticated nature of cyber attacks, companies need to be proactive, ensuring they have the basic procedures in place to protect themselves.

We at Symantec and Deloitte have built our alliance to help companies tackle their cyber security threats today and prepare for tomorrow by helping them make informed decisions about their most important information assets and providing them with guidance and support before, during or after a cyber event.

---

The Invisible Challenge

Against this worrying backdrop, many UK companies feel they are not adequately equipped to deal with the growing threat posed by cyber crime. Our research shows that the majority (60%) of IT decision makers currently do not have the required level of confidence in their company’s ability to effectively tackle cyber attacks.

This is despite the majority of businesses prioritising IT security issues. In fact, 87% of UK IT decision makers place IT security at the top of their agenda. However, the challenge is to ensure this is a priority for the whole business, not just for senior IT decision makers. Our research states that currently under half of all employees in their companies know how important information security is, making this issue a priority for all, from the most junior employee to the CEO.

Lack of confidence in security

- Over half of IT decision makers do not have complete confidence in their company’s cyber security policies
- 6 in 10 do not have complete confidence in their company’s response plan

The majority of IT decision makers are not fully confident that their company has the intelligence and expertise to protect against a cyber attack.

Q1. Which of the following best describes your level of confidence in your company’s policies for cyber security and information protection? // Base: All respondents 505
Q11. Does your company have a response plan in place you are confident in that would be implemented in the event of being the victim of a cyber attack? // Base: All respondents 505
Q7. Do you feel your company has enough intelligence and expertise to protect against a cyber attack? // Base: All respondents 505
“Far too many businesses are unnecessarily at risk as they are not fully equipped to truly understand the cyber threats they face, preventing them from making informed decisions to overcome them”

Andy Ng,
Director and Information Protection Lead, Cyber Risk Services at Deloitte

The challenge for companies, which many are not meeting, is to have a clearer understanding of the risks posed to them and the level of protection needed to combat these threats, in order to inform an effective data protection strategy.

Understand the risks
Our research has uncovered that a key barrier to engagement in data protection is cyber attacks being an ambiguous and an often intangible risk. In fact, 59% of IT decision makers do not think that their company has been attacked, suggesting they are either on the back foot when responding to an attack or do not have the adequate processes to identify such an attack. If the risks are identified and caught early, the impact of non-discriminate attacks such as CryptoLocker (where files on a compromised computer become encrypted prompting the victim to purchase a password in order to decrypt them) can be critically reduced. Understanding these risks is vital to ensure any security detection, prevention or response strategy is targeting the right threats.

Quick wins
But what are the practical steps that businesses and IT leaders need to take in order to get ahead of the cyber criminals? A number of fundamental security procedures, which are often poorly enforced, could represent attainable and immediate wins in the battle against cyber attacks.

Validate your cyber maturity
In order to target the right threats, understand where you are starting from. Determine your current state of information security maturity through qualitative assessments, and against good information security practice, such as ISO 27001, embedded across your organisation.

Quantify your risk
Understand your current risk with quantitative assessments that will validate your current assumptions, as well as build the business case for remediation.

Benchmark your understanding
Encourage communication of cyber issues within your industry network and peer organisations. By sharing information, it will allow you to understand the wider cyber threats posed and approaches to business protection, as well as benchmark your security performance against others.

“Symantec’s Global Intelligence Network has identified a 91 per cent increase in targeted attacks and a 62 per cent increase in data breaches in 2014 over 2013. Cyber criminals have stepped up their game in the past year, yet businesses have not. This latest survey demonstrates there is still a huge gap in security intelligence and understanding by IT managers on how to combat malware and cyber attacks”

Sian John,
Chief Security Strategist, EMEA at Symantec

---

2 Symantec’s Global Intelligence Network (GIN) is a massive archive of security data; we monitor, analyze and process more than 10 trillion security events per year worldwide. Source: http://www.symantec.com/deepsight-products/
The Unrelenting Cost

“Businesses, the Board and their shareholders are vulnerable to the consequences associated with an attack, including loss of revenue, intellectual property, and damage to its external reputation”

Sian John,
Chief Security Strategist,
EMEA at Symantec

In this battle against cyber attacks, many UK companies lack the necessary resources such as specialist expertise or technical data security support. This is despite operating in an environment where being attacked or even raising a false alarm can be damaging.

The true cost of an attack
Our research shows that the 38% of UK companies aware they had been attacked said it had a negative impact on all aspects of their business. These impacts have both short and long term implications affecting their bottom line and reputation.

The true cost of cyber attacks, in terms of economic, reputational and employee impacts, is acknowledged by industry experts as a major concern. And in an increasingly advanced era of cyber attacks, where cyber criminals are often multiple steps ahead, companies are facing an uphill battle. Attackers only need to find one vulnerability to exploit and succeed in their attack, however, businesses must defend their entire estate from potential attack.

This is not helped by a legal environment which fails to deter cyber criminals. In contrast to their victims, who are working against a backdrop of regulation and processes, cyber criminals are currently able to act unfettered by constraints, seeking each and every opportunity to exploit gaps in security process.

This suggests there is still more businesses can be doing to identify ways of improving their data security processes. Despite authorities in the UK and abroad being better equipped to identify attackers and press charges, companies must be responsible for reporting incidents, both big and small. Until now, there has been little incentive for such disclosure, particularly of smaller scale infiltrations.

Cyber attacks can have significant negative consequences on victims

Q17 What kind of negative impact did the cyber attack have on your company in terms of...

// Base: Suffered attack 189

- 79% drop in external reputation
- 78% drop in production
- 77% loss in revenue
- 80% loss in data
- 75% loss of employee confidence
The impact of false alarms

Our research indicates that the consequences of false alarms can be just as damaging to a company. In fact, 4 in 10 UK companies have suffered a false alarm, which can have similar consequences to a real attack, with many citing equally severe consequences for the business from lost productivity hours to reputational impact.

This suggests that the causes of such false alarms, whether these stem from inefficient or inaccurate reporting processes, the incorrect configuration of systems or an immature incident response (amongst others) must be addressed.

False alarms can have equally negative consequences on victims

- **37%** over one third of companies have suffered a false alarm
- **48%** extra large companies (more than 5,000 employees) are the most likely to have suffered a false alarm

Quick wins

- **Plan for an attack or breach**
  
  In order to mitigate the costs of an attack, have a clearly defined incident management ‘playbook’ that allows for effective and efficient incident triage and management. This playbook should be tested on a regular basis with appropriate training for all users.

- **Continuously improve**
  
  No plan will ever be perfect, so seek to continuously improve the process. Document lessons learnt and conduct trend analysis based on the type of cyber event being simulated to refine your incident management processes and the education of your staff.

- **Evangelise the playbook**
  
  Educate not only your key stakeholders but employees at every level on incident management procedures, regularly measuring their understanding and adherence to the playbook.

Q18. Has your company ever had a false alarm where you believed you had been the victim of a cyber attack? // Base: All respondents 505

Q19. What impact did this false alarm have on the business in terms the following? // Base: Suffered a false alarm 189
Many companies at present are not taking sufficient action when it comes to information protection, adopting a reactionary rather than proactive mindset. Our research shows that whilst companies consider various types of information as important, they do not treat them as completely confidential, which is putting hugely valuable internal and external information at risk. For instance, whilst 93% consider customer data to be important, half say that often this information is not treated as completely confidential. This is similar to the perception and treatment of employee data. Understanding how an attacker can use stolen data may give companies an understanding of the value of protecting it and a true comprehension of data protection risk.

Encouraging a more proactive data security mindset requires companies and employees at every level to change the way they view cyber security. Instead of being viewed as a burden to business, embracing the benefits of data security as an enabler of commercial success can be more productive.

New EU regulation coming to the fore in 2015 will impact both companies and cyber criminals alike. In the next year, The European Commission is set to push through its new General Data Protection Regulation (GDPR) reform, and implement a framework designed to transform data governance in the EU. For businesses, this may potentially highlight outdated data processes but more importantly could drive better protection against cyber attacks. Despite cyber criminals becoming more organised, aggressive and proactive in their attacks, stricter data protection processes could be a deterrent.

“The threat from sophisticated cyber attacks continues to increase, along with the repercussions of a breach. It is essential that organisations become proactive and resilient in protecting their business.”

Andy Ng
Director and Information Protection Lead
Cyber Risk Services at Deloitte

Creating a culture of security
Our research shows that IT security decision makers in the UK are most likely to make changes to their information protection policies because of regulation (55%) rather than because of internal values such as company culture (40%). Being one step ahead of upcoming regulation is intrinsic to the fight against cyber attacks.
Building the foundations for resilience

To be sufficiently prepared against attack, companies must improve measures across the board, with less than half considering the majority of cyber protection procedures a necessity.

- **53%** Appropriate firewalls in place
- **45%** Mandatory regular updates to software and patches
- **42%** Frequent password changes
- **35%** Program of checks for devices
- **34%** Regular training for employees

**Quick win**

Implement basic security procedures

Implementing basic security procedures provides the foundation for future security resilience. At present, less than half of IT decision makers that were surveyed believe that regular training, regular device checks and password changes are a necessity. Educate your employees on the value of protecting data and create a company environment which drives a proactive attitude towards data security.

Looking at the measures below that can support cyber security and information protection, could you please say for each one how strongly your company enforces them...

// Base: All respondents 505
Embracing technology

Despite the advancement of cybercrime activity, techniques to fight them are keeping pace. Utilising third parties can capitalise on these techniques, providing effective, predictive measures in the fight against cybercriminals. An external perspective can also help to bring broader threat intelligence and put such threats into a business context.

Utilising third party solutions is just one part of the battle against cyber attacks and there are proactive steps companies themselves can take to control the protection of their data.

We outline three critical areas companies should focus on today to win the cyber war:

• **Knowing your enemy**
  As our research shows, the majority of IT decision makers did not feel that they had been attacked when in reality this is not always the case. Only by understanding the threats posed, through quantifying the risks and benchmarking your understanding of risk, will it be possible to understand the level of protection needed. Knowing the cyber enemy enables easier detection of the threat, increased prevention and a response strategy that targets the right threats.

• **Educating from the inside**
  Cyber security must be a priority for all, not just a few. Companies can do more to educate employees internally, introducing basic data protection procedures such as having regular training programs for employees and frequent password changes. Our research shows that businesses are more influenced by enforced cyber regulation than by their company culture. Driving data protection education from within rather than being led by regulation can ensure businesses are on the front foot of tackling a cyber threat.

• **Implementing cyber resilience**
  Ensuring your company is cyber resilient is as much the goal as cyber crime prevention. Strengthening your security infrastructure with data loss prevention, network security, endpoint security, encryption, strong authentication and defensive measures, including reputation-based technologies will ensure systems and organisations are able to withstand the negative impacts of cyber events.
Methodology
Edelman Berland conducted an online questionnaire amongst IT Decision Makers in the UK on their perceptions of cyber security within their organisation.

How: 15 minute online survey
Who: IT decision makers (IT directors or managers) in companies with over 250 employees
Where: UK
How many: 505 respondents

For more information, please contact:
Andy Ng at Deloitte andyng@deloitte.co.uk or Darren Thomson at Symantec darren_thomson@symantec.com

About Deloitte:
Deloitte provides audit, tax, consulting, and financial advisory services to public and private sector clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has more than 200,000 professionals, all committed to becoming the standard of excellence.

Disclaimer
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

About Symantec:
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared.

The company’s more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion.

To learn more go to www.symantec.com/advanced-threat-protection/ or connect with Symantec at: https://twitter.com/symantec

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

https://twitter.com/symantec
