

Protecting your organisation from itself

The threat from within and how to mitigate it

White Paper



Introduction

In February of this year security researchers proved that with a simple USB drop in a hospital it was possible to hack patient records, critical medical equipment and patient monitors. Vital signs could be manipulated, drug doses changed and medical equipment operated remotely.

In 2015 a Morrisons auditor with a grudge was jailed for leaking personal details, including bank details, of 100,000 other employees. It cost Morrisons more than £2 million to rectify.

US retailer Target lost hundreds of millions of dollars in 2013 when 110 million customers were affected by a breach stemming from a phishing attack on a contractor. Credit card details were stolen as Target's billing system was compromised.

These hacks all have one thing in common: employees.

81 per cent of large organisations that were hacked in the last year stated that the actions of their staff aided the attacker. The 2015 Information Security Breaches Survey from the Department of Business, Innovation and Skills categorically states "People are the main vulnerabilities to a secure enterprise. Respondents believe that inadvertent human error, lack of staff awareness and weaknesses in vetting individuals were all contributing factors in causing the single worst breach that organisations suffered".

Technology can only do so much in protecting a business against a breach when attackers are making the most of employee negligence.

HackTACTICS

Items designed to target employee curiosity.

An example of this type of attack would be leaving items like USB sticks in the path of an employee. These devices can be armed with malicious code designed to disrupt IT services, steal or destroy corporate data.

Phishing.

This is acquiring sensitive information, such as passwords, by masquerading as a trustworthy entity in an electronic communication. Spear Phishing is when this is targeted at a particular individual.

Social engineering.

This involves getting employees to perform actions through a process of psychological manipulation. Social engineering attempts can include a phone call from a hacker acting as a legitimate organisation in order to gain sensitive information.

Online profiles.

More than 600,000 Facebook accounts are compromised every day. Hackers take advantage of employee online profiles; for instance a photo shared on Facebook may reveal their place of work, job role and where they spend their spare time (providing further opportunities for social engineering).

81% of large organisations that were hacked in the last year stated that **the actions of their staff aided the attacker.**



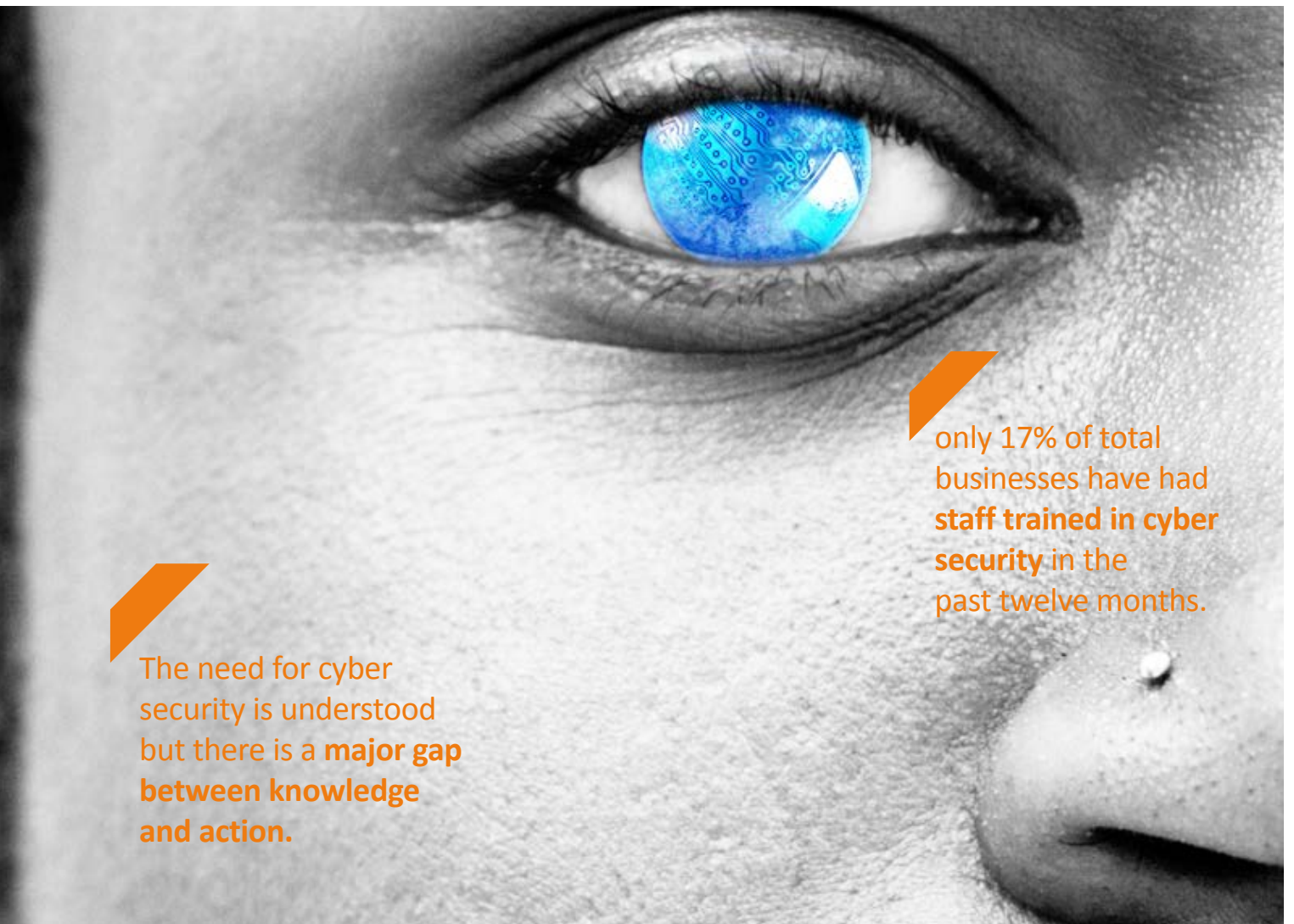
It would seem right to encourage companies to put in place the appropriate protection methods against employee threats. In the 2016 Cyber Security Breaches Survey from the Department for Culture, Media & Sport, 57 per cent of total UK businesses surveyed claimed to have sought guidance on cyber security, increasing to 83 per cent when just polling large companies. The awareness and desire to prevent such breaches is clearly present.

Yet that same report states that only 29 per cent of total businesses polled have formal cyber security policies in place, or have cyber security risks documented in continuity plans or internal audits. On top of this only 17 per cent of total businesses have had staff trained in cyber security in the past twelve months.

The need for cyber security is understood but there is a major gap between knowledge and action. The lack of understanding about how to mitigate against the input of employee negligence is leaving UK businesses wide open to not only the most common type of security breaches, but also the most disruptive and expensive.

Security breaches are now seen by many organisations as inevitable and where the impact has to be prepared for and managed. Others strive for an immaculate record. Both attitudes involve significant investment which can be greatly reduced if your own staff are the first line of defence by default rather than by exception. How can this be achieved? What steps must organisations take in order to prevent their staff from unwittingly (or deliberately) causing a security breach? Their origins can be traced to three distinct areas of a business:

- **Context** – the infrastructure and the workplace
- **People** – staff, HR management and training
- **Security** – digital and physical protective measures



The need for cyber security is understood but there is a **major gap between knowledge and action.**

only 17% of total businesses have had **staff trained in cyber security** in the past twelve months.

Encourage a culture of awareness

Context

If asked, most employees within your organisation would know what to do if there was a fire at work, but would they know what to do if there was a cyber-attack? Policy and procedures provide the framework for safe and secure working and this applies to cyber security as well as physical security measures. As 71 per cent of businesses don't have policies in place, the first step is to set out such processes. But this is by no means the last step. According to the 2015 BIS survey, 72 per cent of businesses where security policies were poorly understood experienced a staff-related breach.


Research undertaken by QinetiQ's human performance experts has shown that employees will often sign/agree to policy documents without reading the contents because they are too long or they do not have the time to read them, leading to situations where staff are unaware of protocol when they are most needed. To combat this, a policy should be:

- Written in plain English. Avoid jargon and ensure it provides context and relevance to staff's day to day lives.
- Easy to implement. Staff are busy, so complex or confusing steps will result in non-compliance or insecure workarounds that bypass the complicated procedure.

- In line with wider business goals and seamlessly fit into its culture. A policy that is at odds with the business that implements it will not encourage staff to comply.

A cyber security policy implemented with these core requirements in mind is much more likely to generate compliance with security.

The balance a job has between its demands and the resources devoted to supporting staff can also impact engagement with procedure. Staff need to be physically and mentally prepared for the work they undertake and motivated to do it properly. If someone is not well-prepared they will not perform to their optimal level so stress and strain should be minimised as much as realistically possible. Also, while policies should be clear on the steps that minimise or deal with security threats, personal autonomy where possible should be encouraged; freedom in decision making increases the likelihood of compliance with protocol.



Freedom in decision making increases the likelihood of compliance with protocol.



Training should be: **Regular, Relevant, Short, Engaging, Empowering**

People

Do employees have the skills required to support the security system? Preparing staff for the role that they will play in reducing human hacks requires investment. Research by QinetiQ has found that although employees often agree that they, as individuals, are responsible for cyber security within their organisations, not all of them feel sufficiently well equipped to protect themselves and the organisation from these threats.

This should come as no surprise. The 2016 Cyber Security Breaches Survey reports that only 17 per cent of UK organisations have provided cyber security training to their staff over the last 12 months. Regularity of training is important. Frequent or refresher sessions containing updates on recent incidents, near misses, policy/procedural changes and threat profile changes are highly effective at drawing attention to the importance and relevance of the topics.

Such training should define the cyber security culture within an organisation, creating a positive social norm as opposed to an atmosphere of non-compliance. Yet it needs to be delivered with the requisite quality to achieve this step-change in culture. Quality training should:

- Be an appropriate length. Consider attention span lengths or other work-related pressures that may detract from full engagement.
- Deliver the correct content in a way that engages appropriately. It should be relevant to the job role of those in the training, both in the amount of prior knowledge needed and how cyber security is related to their job.
- Have clear outcomes. Good training will make it clear to employees what is expected of them and positively impact their conduct.
- Use real life examples. Studies have found that 94 per cent of staff changed the way they thought about security after hearing a story about an incident and 52 per cent changed their behaviour.


The length, content, outcomes and examples used in training should be directly linked to the behaviours the business needs to change.

One of the most common behaviours that leads to a security breach is called a 'workaround'. These are methods created to accomplish a goal within a system of dysfunctional processes that prohibits or makes the accomplishment of that goal difficult (e.g. it requires more effort to do a task than it first appeared). Personnel often feel that the risks posed by workarounds are low-level risks likely to cause embarrassment. However, they often have the potential to cause disruption to an organisation's processes and therefore open up a vulnerability in security.

Common workarounds to be discouraged include:

- Sharing log-in details/passwords
- Writing passwords down or using simple letter and number combinations
- Emailing documents home to work on using their own equipment

The ease with which computers and other systems can be used impacts on compliance to such a degree that tasks that are not user-friendly will be ignored or avoided, meaning that security practices may not be followed. Training can be crucial here to instil the reasoning behind such processes. But equally, the tenets for a good security policy can be applied to work security systems; if they aren't easy to understand or implement, they may well fail.



'Workarounds' are one of the most common behaviours that lead to a security breach.

Focus vigilance where it is most needed

Security

We've heard from the government on how people and employees can impact a business, with average costs of up to £1.15m cited. That doesn't mean it would impact all businesses in such a way, but the nature of breaches makes scenarios very hard to predict. Human error can happen in all areas and at all levels of a business, opening up both digital and physical arenas to compromise. So how does one start to assess where and how to improve technical and physical security? Again, understanding human behaviour should guide these security processes.

- **At what level are security policies and protocols followed best?**

Junior staff, thanks to regular training, can often be the most security conscious staff members. Those higher up may not be aware of new threats and protection policies in place. At the same time, senior staff are more likely to have 'skin in the game' and so will be more aware of what can go wrong if processes are not followed.

- **Do distinct departments or sites differ in compliance with policy?**

If an organisation is large enough, visibility of threats can be different depending on job roles or physical location. For example, those in an IT department, or closely linked to one, may understand the impacts of network or communications breaches more than others and so adapt their behaviour accordingly. Similarly, warehouse operatives or facilities support staff may be more aware of vulnerabilities in physical access systems.



Assess security processes from the employee's perspective

- **Are there staff that already perform to a 'gold standard'?**

Identifying business areas where security is optimal will save significant investment, ensuring resources are focused on improving the behaviour of those that need it most.

Understanding this landscape will then guide where training and policy changes need to be made. However, that shouldn't be considered 'job done'. Whether the changes are having the desired impact still needs to be ascertained. To do this, you need to measure the following:

- **How are security procedures performing after training or policy implementation?**

An assessment method needs to be in place to understand how the new security structures are performing, with a suitable metric that shows where performance is good or bad.

- **Are there sections of the workforce that require more training than others?**

Training methods influence people differently. It is worth reviewing how new policies and processes are taken up across departments, hierarchies and long and short term employees to identify areas that need alternate approaches.





Effective cyber security is a combination of **good technology** and **good practice**.

Take home message

The 2016 Cyber Security Breaches Survey contains not just hard facts about the effect of employee behaviour on breaches but also reveals a positive, wider sentiment among business leaders that points to a security conscious future. In short, it found that businesses understand that cyber security is a good practice issue as well as an IT problem.

Yet these positive findings are not resulting in secure businesses. A key reason for this is because technology alone does not deliver security. The three step process laid out in this white paper - the same followed by QinetiQ's Human Performance Team through its Security Culture Assessment Tool - can bridge this gap:

1. Develop processes that create a business **context** of secure staff behaviour.
2. Make sure **people** can follow these policies.
3. Focus on **security** awareness and vigilance where it is most needed.

By basing internal security strategy around these issues employees will be motivated to remain alert to risks and unusual behaviours, will be more engaged and productive, and businesses will be more secure as a result. This will restrict the easiest route - the main vulnerability, as described by the Government - of breaking into a UK enterprise, protecting the country against some of the most damaging attacks yet seen.

If you would like to know more, please contact:

Simon Bowyer,
Senior Consultant,
Human Performance,
QinetiQ

01252 397899

SJBOWYER@qinetiq.com

Natalie Fisher,
Senior Consultant,
Human Performance,
QinetiQ

01252 392990

NFisher2@QinetiQ.com

QinetiQ

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom
Tel: +44 (0)1684 894750
Email: cyberteam@qinetiq.com

www.qinetiq.com

QINETIQ/16/02495

© QinetiQ Ltd 2016

QinetiQ is a trade mark and registered trade mark
of QinetiQ Limited in the EU, US and other countries.

The QinetiQ logo is displayed in a bold, blue, sans-serif font. The letter 'Q' is significantly larger and more prominent than the other letters, which are in a smaller, uniform size.