

A BoxingOrange publication

SecurityMatters

Summer 2010

In this issue:

**Getting to grips with
Cloud computing**

Why and when to bring in
a security expert

**The DPA has grown teeth –
how to avoid getting bitten**

Why we need the people
as well as the technology

A hand is shown from the right side of the frame, holding a small piece of white paper. The paper has the text 'Keeping one step ahead of the bad guys' written on it. The background is a light blue circular graphic with a white center. The text 'bad guys' is in a large, bold, dark blue font, while 'Keeping one step ahead of the' is in a smaller, teal font. The hand is positioned as if it is about to tear the paper.

Keeping
one step
ahead of the
bad guys

Understanding the changing
landscape of **information**
security threats

Putting **Information Security** into perspective for **your business**



Phillip Ineson



Kirsty Cowan

"It takes a progressive and open leadership to proactively request independent feedback from your most important audiences."

Security Matters Summer 2010

Contents

- 03 **Looking to the future** It was time for change at Boxing Orange
- 04 **Behind the screens** Why we need the people as well as the technology
- 06 **Putting our partners through their paces** It's all about commitment
- 07 **Caught in the act of protecting data** The DPA has grown teeth
- 08 **Why bring in an expert?** What's in it for me?
- 10 **Staying one step ahead of the bad guys** How do we out-think the enemy?
- 11 **News** Updates from Boxing Orange
- 12 **Stacking the odds in your favour** Sector spotlight: Gaming and online betting
- 13 **The perfect platform** Our partnership with ArcSight
- 14 **Taking our heads out of the clouds** Getting to grips with Cloud computing

New Business Wins

- Managed SIEM Deployment for:**
A leading online betting organisation
A UK Government department.
- Managed Firewall Service for:**
A UK banking group.
- DDoS Mitigation for:**
A leading online betting organisation.
- CLAS Consultancy for:**
A UK Government department.
- Managed IDS for:**
A European investment house.
- PCI DSS Services for:**
A leading UK retail organisation.

Hello and welcome to the Summer 2010 issue of **Security Matters – Boxing Orange's industry journal**. This time last year, cost savings and ROI featured heavily in our publications, reflecting the challenging times many organisations were, and still are, facing worldwide. Even before the recession hit, we at Boxing Orange were focused on improving productivity and efficiency, without compromising the quality of service we provided.

Thanks to the superb efforts of our team, who have worked closely with our clients to deliver even more tailored solutions, we have enjoyed a year of financial growth. This is testament to the hard work and dedication of all involved, despite difficult economic times.

Underpinning our success has been the strength of these ongoing client relationships, which have allowed us to continue investing in key technologies and, more importantly, people. It gives me great pleasure to welcome specialists Martin Dipper, our new Director of Security Services, and John Ellerton, who joins us as Business Development Manager, to work with clients and identify opportunities to support their organisations further. Both men bring vast experience to Boxing Orange and I wish them well in their new roles.

As well as expanding our team, we have been working closely with our professional partners. As Webscreen Technology's Premier Partner, we helped celebrate their 10th anniversary in May. The event gave us the opportunity to thank Webscreen for continuing to provide exceptional service, growth and delivery of an award-winning DDoS Mitigation platform that many of our clients rely on.

In addition, having successfully deployed ArcSight's SIEM award-winning technology as a Managed Service for a number of key clients, we have been able to reflect on the exceptional benefits the solution has provided. As a result, we have committed to ensuring all our clients benefit from this industry-leading platform, which we see as the foundation for all security needs across our customer base. The diagram on the back cover illustrates this in more detail.

Our position as sector experts has been further strengthened by our invitation from the House of Lords Select Committee to contribute to a report entitled 'Protecting Europe from large-scale cyber-attacks.' Following this, Boxing Orange was also highlighted as a World Wide Service Provider in Forrester Research Inc's March 2010 report on the Managed Security Services Provider (MSSP) market, which examines the growth and potential of the market, and the reasons for its development over recent years – another great result for our business and our clients.

Moving forward, as cutbacks in the public sector seem set to continue, we predict that an increasing proportion of the clients we work with will be within the private sector.

Our autumnal agenda of roundtable events will reflect this. As Data Loss Prevention (DLP) is high on many of our clients' priority lists, we will also shortly be announcing the launch of a new DLP Managed Service, together with additional Database and Application Security Services.

Finally, I'm thrilled to say that due to our strong current financial standpoint, which is the result of our effective long-term customer relationships, we are actively engaging with like-minded security companies within Europe to discuss potential acquisition opportunities. So watch this space for an announcement in the not too distant future.

I hope you find Security Matters an informative, thought-provoking and interesting read, and I look forward to hearing your comments or ideas for future issues via the feedback form on our website.

Phillip Ineson, Co-founder, Boxing Orange



Even in a relatively 'young' sector like **Information Security, standing out as different and relevant in what is fast becoming a commoditised marketplace is a challenge, particularly for smaller organisations. This is made even harder by customer confusion as the market moves at an increasingly rapid pace and new developments appear almost daily.**

At the end of last year, the Directors at Boxing Orange felt it was the right time to independently review their own brand's positioning, performance and profile. Their aim: to ensure they remained relevant and compelling to their existing customer base, as well as engaging for future prospects and business partners. So they gave us at Propaganda a ring.

Propaganda is a management consultancy that specialises in brand strategy and implementation. We work with business owners across multiple sectors to help them develop effective positioning and communications that deliver relevant brand promises for customers, partners and employees. Which is exactly what Boxing Orange needed to really maximise the potential of their business.

Discovering Boxing Orange's difference

From the outset, it was clear that Boxing Orange had a close affinity with its customer base and business partner network, with a team that held excellent knowledge and industry-leading experience and qualifications. However, we knew we should make no assumptions about the Boxing Orange brand or its position in the hearts and minds of its key stakeholders. In short, we needed to gather knowledge and deliver business insight into where the brand should go next.

We embarked upon a programme of Discovery to put our principle of 'knowledge before assumption' into practice and utilise brand research techniques to gain a clear perspective of the brand's positioning in the eyes of its key stakeholders and audiences.

For Boxing Orange, Discovery involved a 360° review of the business and its market context. We interviewed a sample of staff, business partners and most importantly, customers, to gain their feedback and perspectives on the present and their aspirations for the future.

So, what did we learn? An opportunity to get closer to customers

Our research demonstrated that, while Boxing Orange had a solid understanding of customers' businesses from a technical perspective, there was a significant opportunity and increasing need to better understand their business strategy, objectives, long-term ambitions and ongoing challenges. In light of this insight, Boxing Orange has introduced a new approach and process that supports all teams, particularly commercial and technical, to engage in more thorough strategic dialogue.

Raising the profile of security

You only have to open the morning newspapers to see that Information Security breaches are becoming a far more serious threat to business performance, reputation and customer experience than they were even five years ago. However, our research showed that there is an ongoing challenge to get the issue onto the corporate agenda. From a customer perspective, Boxing Orange has a permissive role to play in raising corporate awareness of the importance of a proactive, rigorous and future-focused security strategy to Board members and senior decision-makers within organisations.

A new proposition

So what of the brand positioning for Boxing Orange? The strongest and most valuable brands in the world are single-minded about the benefits they bring to their customers and people. While Boxing Orange remains a comparatively small, specialist business in the broader MSSP marketplace, Discovery demonstrated that customers believe it has a clear difference and an important role to play in protecting and planning their future security landscape. Boxing Orange is seen as an agile, expert and flexible business that can deal with the ever-changing information security challenges customers face. While no organisation has a crystal ball to predict the future, customers believe the Boxing Orange team have the

knowledge, resources and expertise to design and deliver security solutions that will future-proof corporate reputations and performance.

The new brand proposition, 'Tomorrow's Security Today', and supporting visual identity, are a direct articulation of a clear and strongly-stated customer need, coupled with a belief about the Boxing Orange difference. It has now been explored and embraced by every member of the Boxing Orange team and will be the driving principle as the business moves forward.

A brand of the future

Embarking upon such a programme is no mean feat for any business. It takes a progressive and open leadership to proactively request independent feedback from your most important audiences. And it takes courage to listen and learn from the feedback, then actively address issues and opportunities. A strong and successful brand is not created or established overnight, and over the coming months there will be significant time and effort devoted by both the team at Boxing Orange and the team at Propaganda, to ensure the new brand is delivered effectively to stakeholders in every area of the business.

So watch this space. Because 'Tomorrow's Security Today' is not just an idea – it's a promise.

Propaganda's Brand specialist, Kirsty Cowan, explains why Boxing Orange felt the time was right for a total brand review, and how what they uncovered will revolutionise their business forever

Looking to the future



Stuart
Williamson

“However advanced your system, it seems **there is no substitute for the human touch.**”

As they evolve, Security Information and Event Management (SIEM) systems are becoming increasingly complex and capable. As a result, many vendors are promoting their vision of an automated system – a silent partner that detects malicious behaviour and automatically makes changes to your network to minimise attacks. However, letting a rule-based system make critical changes to operational infrastructure without any human intervention is a scary prospect, and a step too far for many organisations.

Quite often, SIEM system rules are written with a limited understanding of the wider information security landscape and the client’s specific baseline. Without this awareness of the context, the system can only react to problems as they happen, not be proactive in avoiding them. Which means you’re never as protected as you could be.

Using specialist security analysts to interpret SIEM information enables a much ‘bigger-picture’ approach. Additional information feeds can be used to increase the contextual understanding of any particular security threat. Without this layer of human intelligence, SIEM systems can be relied on too heavily and the value of the information they produce is reduced.

Analysts act as technical translators or interpreters for their clients; they not only understand the security language, they understand security culture and risk. Placing analysts between you and your SIEM system means there is always an added level of intuition and insight to help you understand issues and assess risks much quicker than if you simply interfaced directly with the SIEM system. However advanced your system, it seems there is no substitute for the human touch.

Who + What + Where + When = How + Why

With new security vulnerabilities surfacing daily and the rate at which they appear increasing, knowledge of the most recent security threats is vital if you are to keep pace in the security arena. Today’s appliances, servers and software all have the ability to log detailed security information that can be used to monitor overall security, but the volume of data is often too overwhelming for human analysis. The goal of security management, therefore, is to define, and ultimately obtain, a true and verifiable record for any single security event. This almost-forensic process, which includes data collection, information processing, knowledge collection and deductive processing, turns information into intelligence.

Having automated systems and technology to tackle this sea of information is essential, but as the data is processed the analyst’s role becomes more and more important. Without them, every situation can only be addressed based on the information presented. In contrast,

the multi-faceted and distinctly human brain of the analyst uses historical information, shared knowledge of other analysts, vendors and specialist security information to identify potential threats and devise individual solutions. So it is important that Managed Security Service Providers (MSSPs) encourage their analysts to work as a team, sharing their knowledge and previous conclusions.

It’s good to talk

As well as historical time-based logs of all incidents that are thrown up from the automated data collection, known as trouble ticketing tools, internal collaboration tools such as bulletin boards, wikis, email groups and forums are great ways for analysts to communicate knowledge, deductions and conclusions. As these tools are internally-based and secure, they allow the free flow of knowledge between individuals who may not physically meet due to shift working patterns. They also enable searching and historic ‘threading’ of key topics, making them more appropriate mediums for discussing background issues and security alerts, sharing conclusions and spreading best practice.

Testing, testing, 1, 2, 3...

Opting for an MSSP rather than a purely automated system means you can be confident that when someone is attacking your core infrastructure, you will know about it. Within minutes, an analyst from the MSSP will have alerted you, identified the attackers and determined what they are doing. And if it turns out the attack was actually a test performed by an outside agency that audits your network, you have got the intuition and responsiveness of the individual specialist to thank.

This example demonstrates one of the key benefits of using an MSSP to manage security – to respond quickly and effectively, the process relies on the intelligence and response of actual people, not just technology. Information Security is about good process operated by good people, as well as good technology. It is true that technology has a vital role to play in sorting the wheat from the chaff, but the process of achieving a true and targeted response is all about people.

People who see, people who do

Too often with automated systems, valuable alerts from firewalls, servers, and even IDSs are simply ignored. However, trained experts can actively look for signs of attack. Understanding the client’s environment is a key factor in this, as establishing a context for the security information that’s being monitored enables a much more proactive approach. Having said that, it is not enough to simply detect attacks. Again, the human element is vital as analysts can actively assist with closing vulnerabilities when attackers find them, as well as investigating incidents, and helping prosecute attackers.

“Knowing your business is being protected by more than just technology, that there are people at the end of the phone watching your back 24/7, definitely makes it that bit easier to sleep at night.”

Security management requires continuous monitoring and education, which clients often don’t have the resource to achieve internally. MSSPs on the other hand are in constant contact with security teams and vendors, to educate their analysts about new attacks as soon as possible. They also work closely with vendors to install security patches and upgrades the moment they are available or needed.

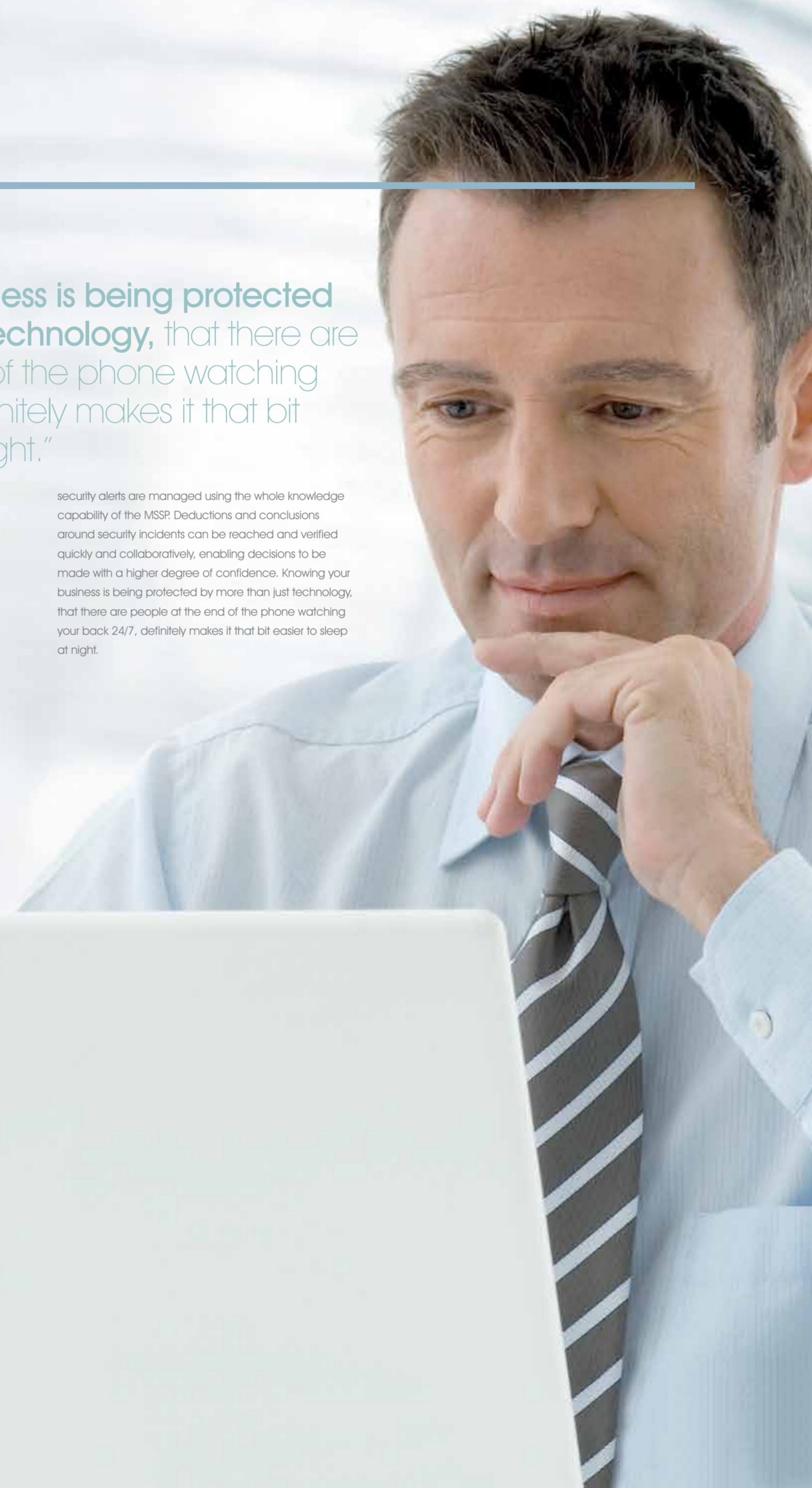
security alerts are managed using the whole knowledge capability of the MSSP. Deductions and conclusions around security incidents can be reached and verified quickly and collaboratively, enabling decisions to be made with a higher degree of confidence. Knowing your business is being protected by more than just technology, that there are people at the end of the phone watching your back 24/7, definitely makes it that bit easier to sleep at night.

A few final thoughts

There is no doubt that as organisations become more aware of their security requirements, the security event information they need to harvest is increasing. The role of technology in processing this vast amount of data is important; however, the analyst is fundamental in turning this data into intelligence. Using a blended approach of technology, process and analysts means that

Behind the screens

Stuart Williamson considers why we need the people as well as the technology





John Dyson

“Only those who demonstrate exceptional ability are selected to become an official Boxing Orange vendor.”

Putting our partners through their paces

Being such technical specialists, love at first sight isn't a concept we place much faith in – or, in fact, any. John Dyson explains why we insist on knowing everything about our partners before we will consider making that commitment.

When it comes to selecting vendor partners, we are anything but an easy first date. We take the selection process very seriously; so seriously in fact that we have developed a robust five-step approach that ensures we only partner with the right suppliers to meet our clients' needs. Here is an insight into the criteria behind those decisions.

Step 1 making sure we know exactly what we want

Before we start talking to potential partners, we ensure we have a clear and detailed understanding of exactly what it is we are looking for. To do this, we put together an internal evaluation team to define our needs, based on our clients' requirements, in terms of product, service, technical capability and commerciality. Once this has been hammered out, an outline document is produced and circulated to our Challenge Team to validate. If everyone is happy that we have everything covered, the search for the ideal vendor begins in earnest.

Step 2 finding the perfect prospective partner

With such exacting criteria, we know that not every vendor will meet all of our requirements, so if necessary we will request further information from those we want to know more about. As we believe in the importance of a human

approach, we let our analysts review this information and assess whether they believe the vendor is right for our clients and our businesses. Those that are selected are then asked to provide a more in-depth overview of their credentials, project history and accreditations. Once all of this information has been gathered, we evaluate them and draw up a shortlist of potential candidates. If you are thinking that such detailed screening must be time-consuming you'd be right, but by being so thorough at this stage, we can be confident that everybody involved understands what is expected.

Step 3 getting down to detail

To make sure potential vendors know the specifics of what we expect of them, we prepare and issue them with a brief detailing exactly what it is we're looking for. As well as the technical requirements of the product or service we want them to supply for our customers, we also ask them to present details about their business, their processes and their experience, so we can assess whether their way of working aligns with our own.

Step 4 marks out of 10

As we believe in making objective decisions based purely on fact, our judgments have to be backed up by proven capabilities and results, rather than hype. To do this, we look at each of the requirements we have asked the candidates to fulfill, and assign an importance value

for each one, based on the business needs of both ourselves and our clients. We then rate the performance of each potential partner against these. Only those who demonstrate exceptional ability are selected to become an official Boxing Orange vendor.

Step 5 shaking hands on a bright future

Once we have delivered the good news, we set about building a long-lasting relationship with our new partner that's founded on trust and honesty from day one. Together we agree on objectives and priorities, and consider each project from every angle, to ensure all potential challenges are highlighted and assessed. The keys to any successful partnership are effective communication and shared goals, so we work hard to establish working practices that are an effective solution for both parties. Our people get to know their people and the partnership begins to grow and evolve.

By striving to get it right from the outset, everyone involved can look to the future with confidence. So there you have it: by making sure we are always proactive and rigorous, we can guarantee that every Boxing Orange partner rightfully earns their status. You can be confident that together, we will always deliver quality, value and competitive advantage for your business.



Dave Ward

“With this most recent change providing the Data Protection Act with real teeth, can we really now afford to ignore this legislation?”

Caught in the act of protecting data

Dave Ward unravels the implications behind one of the industry's most misunderstood areas

In today's business environment there is a plethora of governance and security standards – PCI-DSS, Sarbanes Oxley and HIPAA to name just a few – which organisations have to address and adhere to. However, there is one piece of legislation that is often misquoted, misunderstood or completely ignored – the Data Protection Act.

Let's rewind 10 years... The Data Protection Act (DPA) 1998 came into force on 1 March 2000 and replaced the Data Protection Act 1984. The Act provides individuals ('data subjects') with a general right of access to any 'personal data' about themselves held by 'data controllers' within the United Kingdom, as well as laying down principles for the way personal data must be managed.

The 'data controller' is the person or department within an organisation that determines the reason for holding and processing personal data, and the nature of that processing. The Inland Revenue is one example of a data controller.

DPA – the basics

The Data Protection Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, to ensure that personal

information is (1) fairly and lawfully processed, (2) processed for limited purposes, (3) adequate, relevant and not excessive, (4) accurate and up to date, (5) not kept for longer than is necessary, (6) processed in line with your rights, (7) secure and (8) not transferred to other countries without adequate protection.

The second area covered by the DPA provides individuals with important rights, including the right to find out what personal information is held on computers and most paper records. Should an individual or organisation feel they're being denied access to personal information that they're entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office (ICO). Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

How do you know if you're getting it right?

So now we know what it is and what it covers, the next thing to consider is how it affects your organisation. The DPA doesn't guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals and the sometimes-competing interests of those with legitimate reasons for using personal information.

Not sure if your actions comply with the DPA? Then follow this short checklist:

- Do I really need this information about an individual?
- Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I were asked to pass on personal information, would the people about whom I hold information expect me to do this?
- Am I satisfied the information is being held securely? What about my website? Is it secure? Is access to personal information limited?
- Am I sure the personal information I hold is accurate and up to date?
- Does my organisation have processes in place to delete or destroy personal information as soon as I have no more need for it?
- Has my organisation trained the staff in their duties and responsibilities under the DPA, and are they putting them into practice?

The power behind the principles

Fail to meet the above requirements and your business can quickly come under scrutiny. The ICO has far-reaching legal powers to ensure all organisations comply with the DPA. To do this, they undertake audits to assess whether those processing personal data follow good practice. They also conduct assessments to check organisations are complying with the Act, and serve information notices requiring organisations to provide them with specified information within a given time period.

Where there has been a breach of the Act, the ICO can serve enforcement notices and 'stop now' orders forcing organisations to take remedial action to ensure they comply with the law. In more serious cases they also have the power to prosecute those who commit criminal offences under the Act, and can report to Parliament on data protection issues they believe to be of concern.

A costly mistake to make

Following a number of well-publicised incidents within the UK, the penalties for failing to comply with the DPA have recently been reviewed, and from 6th April 2010 the ICO was granted new powers to issue notices requiring organisations to pay up to an eye-watering \$500,000 for serious breaches of the Data Protection Act.

With this most recent change providing the Data Protection Act and the Information Commissioner's Office with real teeth, can we really now afford to ignore this legislation?



Martin Dipper

“Choosing your provider wisely can not only save money in the short-term but also help achieve a better return overall.”

With so many budgetary pressures on today's businesses, using an outsourced service can often be a difficult proposition to sell in to the board and C level executives. But what many organisations fail to realise is that choosing your provider wisely can not only save money in the short-term but also help achieve a better return overall, as well as preventing considerable losses and embarrassment further down the line.

When choosing your provider, remember – you are entering into a trusted partnership that offers clear benefits for your business. Chances are security is not one of your organisation's core competencies, so outsourcing repetitive and technically challenging security functions can be incredibly advantageous, in terms of headache reduction as well as financial benefit. Not only will it strengthen security, it can help you avoid escalating internal costs, potential reputation damage, loss of productivity and intellectual property theft. By outsourcing to the right expert partner, you can be confident you've got compliance issues covered, allowing you to focus more on your day job and doing what you do best – running your business.

Here are just a few more immediate benefits of using an MSSP:

Reducing the risk

The real-time monitoring of security devices, servers and IT systems by security experts means malicious activity and emerging security events are always identified and prioritised. As a result, you can make quicker, more well-informed decisions to reduce corporate exposure, minimise business interruption through the protection of critical assets and reduce the number and impact of attacks.

Getting more from what you've got

I'll be the first to sing the praises of security devices, but they can create large volumes of data that often overloads internal resources and is difficult to understand. As well as being costly and time-consuming, this can lead to missed threats and attacks if the data is not adequately reviewed. But opting for a mature and scalable security platform provided by an MSSP enables you to exploit the full functionality of existing technology and gain visibility into the real threats while reducing information overload.

Cutting costs without compromising

To run a full-time, in-house security monitoring team is expensive and very hard to maintain. By partnering with a flexible MSSP, you get the benefits of using a professional Security Operations Centre (SOC) team, and the associated

results, for far less outlay. You'll also receive a consistently high quality of service and a reduction in the time and cost spent analysing security risks internally. This lets you actively take control of your staff and your operational security costs, allowing you to focus resources on strategic issues.

Advanced warning of threats and data insight

A significant reason for choosing a MSSP is the scalable and state-of-the-art systems they'll have in place for collecting and analysing data. Their thorough security event correlation and data-mining features will enable analysis of security data faster and more accurately than you could realistically achieve in-house. What's more, they'll also be able to provide the context behind the events, to aid correlation with the customer environment and emerging threats.

A 24/7 solution

We all know that determined attackers don't choose the most convenient times to attack. In fact, they usually choose the most inconvenient (for you); often over the holidays or when internal staffing is at its weakest or non-existent. Choose an MSSP and your team never goes home; it's operational 24 hours a day, 365 days a year. So it's always there when you're not. Expert SOC staff view traffic from multiple customers from all parts of the world, giving them unparalleled visibility into threats and events, often before they affect your environment. They're able to separate actual security threats from false positives, with reliable results, delivering incident alerting and

incident management. Again, this provides you with a level of security expertise that is difficult to source and maintain in-house.

Help managing your security devices

As well as security logging and monitoring services, a good MSSP will provide remotely-delivered management services for supported security devices. And because they'll deliver Change Management, Release Management (software, OS & patch maintenance) and Fault Management for customer devices anywhere in the world, you can free up even more internal resources.

Complete compliance

Compliance with industry standards and regulations is something we're all tied to, and is essential for not only staying in business but also generating customer and partner confidence too. Some countries and US states are now wrapping regulations in law, meaning that a fine can be followed by more serious penalties. Professional 24/7 monitoring and management ensures your business is always compliant, so you never risk getting on the wrong side of the auditors.

In-house consultants and Professional Services

Another thing to consider when selecting an MSSP is whether they offer integrated Professional Services to help implement services and provide ongoing maintenance and management. An established MSSP will be able to offer penetration testing, compliancy assessments and project management and implementation services. It's important that these consultants are part of the same services team and are not shipped in from a third party or another location within the MSSP's business. Why? Because you need to know you're paying them to 'do', not to learn about the service being implemented.

Don't forget, it's vital that you regularly review your MSSP to ensure it's fit for purpose. Many MSSPs have spent a decade building operational systems and business strategies that are focused on perimeter and network security. But the attackers have realised this. As a result, threats are changing from traditional network-based attacks to application-based attacks. Many of the biggest compromises have occurred because companies and their service providers have been busy watching the network and perimeter, and have taken their eye off the database and application layer.

Looking to the future

I recommend you find a provider that can supply what Forrester calls SOC 2.0 operation. SOC 2.0 is not built around big projection screens and network technology; it's built around Security Information Event Management (SIEM) tools and log management. It has the ability to collect and analyse logs from all customer devices easily, using one core technology. SOC 2.0 will move from being focussed purely on security devices to a larger concentration on all customer devices and applications with links to compliancy. Many MSSPs with legacy setups are struggling with this concept.

Fortunately, Boxing Orange customers have no need to worry. Our SOC is already operating on SIEM SOC 2.0 technology, allowing us to expand and support new devices as our customers grow and the threats change. By delivering real-time security protection, helping organisations demonstrate compliance, and reducing overall security risks in the face of today's emerging threats, we're helping future-proof our clients' businesses.

“Not only will it strengthen security, it can help you avoid escalating internal costs, potential reputation damage, loss of productivity and intellectual property theft.”

Why bring in an expert?

Martin Dipper considers the ‘what's in it for me?’ angle of opting for a managed security service





Dave Ward

“A strategic approach means you might never have to go to battle in the first place.”

Staying one step ahead of the bad guy



When it comes to protecting our information, Dave Ward considers – how do we out-think the enemy?

Since the beginning of time, man has coveted the possessions of his neighbours. As a race, we have plunged the depths of deceit and deviousness, beyond even those used by Machiavelli himself, to devise evermore cunning ways to accomplish this.

In days of yore, protecting our possessions was achieved by a show of strength – the stronger you were, the less likely it was you would become a target – but even overt displays of strength wouldn't stop the truly envious or greedy, or those skilled in the ways of Machiavelli. So we learned to adapt and started using the same methods to protect our possessions as those attempting to take them. We learned that stealth was often better than overt action, and that thinking like the enemy and anticipating their moves allowed us to mount the best defence.

So can we learn from the lessons of the past, and use what our ancestors knew to help protect our possessions in the high tech world of today, and more importantly, tomorrow? Specifically, to protect arguably the most precious thing we own, our personal information; the loss of which causes us more pain and problems than anything our predecessors could ever imagine. Apart from maybe a well-timed swipe from a broadsword...

Don't think – know

Of course, understanding what a modern day attacker wants – access to our information – and how they are going to achieve this, is paramount, but it's only the first step. Without this understanding, and without undertaking a thorough analysis of the threats, those of us responsible for protecting data could well be spending money in the wrong place and at the wrong time. The cold hard reality is that as the world recovers from a recession, no-one has an endless supply of cash to spend, and most of us are seeing our budgets being heavily cut. This time, the broadsword is swiping from within.

Are you leaving yourself open to attack?

I say 'of course attackers want access to our information' as if it was obvious; but if it is obvious, why do so many of us not understand it or indeed act upon it? Why do we hear stories every day about this laptop or that memory stick being left on the tube or in a taxi, or personal information being emailed to the wrong person? Is it that we just don't understand where the threat to our information comes from, or that we don't have the time to do anything about it? Or even worse, are we just hoping that it won't happen to us?

If this essential risk analysis is flawed, or not even carried out, then we run the risk of defending our data against an attack that could never happen, whilst forgetting the obvious ways in which our data could be lost. Get this wrong and the impact upon the business we are protecting may simply be seen as an embarrassing blip that temporarily reduces the capability of the business to service its clients. Arguably this could be classed as a minor consequence that most organisations, given time, could overcome. With the public expectation that personal data is sacrosanct, plus the increased power of the ICO to issue fines of up to £500,000, how many organisations would be forced into a downward spiral from which there is no return?

The power of expert insight

There is no denying the fact that understanding the threat landscape is a time-consuming process. Not every organisation has an IT Support team with the time, ability or objectivity to undertake this task, which is why it's often either forgotten or ignored. But ignorance is not defence, and this lack of resources is not an acceptable reason for not adequately protecting personal data – just ask your clients. So utilising the services of a professional security company to provide a robust risk analysis and a comprehensive mitigation plan is a great way to bridge this gap.

Critical balance

Maintaining the appropriate balance between the value of the data we need to protect, and the cost of that protection, is a juggling act that Security Managers face each and every day. I say hats off to them, our silent protectors tasked with keeping all the balls in the air while simultaneously responding to requests and demands from their audience at large, and all the while maintaining a cool, calm persona that makes it seem effortless. At least in the most part.

“Where do I spend the budget I've got, in order to provide the best protection?” is the most common question I hear when discussing security with clients. The answer should always be to firstly understand the threats to the data you are protecting, as only once you've achieved this level of understanding can you plan and cost an appropriate defence.

The Holy Grail?

With this in mind, Boxing Orange has developed an innovative process – the Go-Model.

The Go-Model is a structured process that allows Boxing Orange to develop a security strategy based on our clients' unique business environments and the challenges they face. Through this 9-stage process, we can help any organisation understand the IT risks that they are currently exposed to and provide a roadmap towards mitigating those risks.

How do you out-think your enemies? Choose a security provider that's more than just a knight in shining armour. Because a strategic approach means you might never have to go to battle in the first place.

Introducing our innovative automated scanning tool

Boxing Orange is proud to announce the addition of an automated scanning service to our Professional Services portfolio. Powered by Qualys Inc, the cutting-edge service provides fully-automated network scanning and high quality, easy to interpret reports. Great news for businesses of all sizes, it'll help our clients achieve and demonstrate PCI DSS Compliance.

It does this by generating ASV reports that allow organisations to meet the quarterly security scanning requirements demanded by major payment-card brands, giving them total confidence that their environment meets strict Payment Card Industry Data Security Standards (PCI DSS).

What really makes the service stand out is our use of 'plain English' explanations for what are sometimes quite complex issues. By providing a human touch throughout the process, our experienced analysts can interpret the exact implications of the results that are generated.

The new service will give clients 24hr access to their own highly-skilled virtual security team, who will be constantly probing their network to discover vulnerabilities and identify risk. All problems will then be rated and reported, together with a recommended remediation plan. By acting quickly and effectively, we'll enable organisations to protect their assets and keep their businesses running, while maintaining the highest levels of security at all times.

To find out more about Boxing Orange's Scanning Services, please contact us on 0113 232 2330 or email: pci@boxingorange.com to discuss your requirements with one of our in-house security specialists.



Welcome to our new Director of Security Services

Martin Dipper is responsible for driving the portfolio and roadmap of security services and the daily operation of the security services teams. He has strong experience in security operational management, service management, vendor management, customer management and delivering leading-edge services that support the needs of large corporations.

Prior to joining Boxing Orange, Martin held a number of vice president and general manager roles in IT security companies, such as Symantec, Vistorm (EDS) and Infonet (BT), along with corporate consulting positions at Microsoft. His expertise is focused on building and managing services portfolios, delivering 24/7 support desk services and supporting dashboard tools to customers.

Martin has extensive experience in managed services, having been in this field since 1994 and specifically in security services since 2000. He is an avid classic car collector and is a member of the Aston Martin owners club. Additionally, he reads theoretical physics and cosmology. We would like to take this opportunity to welcome Martin to Boxing Orange.



Boxing Orange employees are top CLAS

We are delighted to announce that a Boxing Orange employee has recently gained CLAS accreditation.

CLAS is the CESG Listed Adviser Scheme – a partnership linking the unique Information Assurance knowledge of CESG with the expertise and resources of the private sector.

Developed as a result of the increasing awareness of the threats and vulnerabilities that information systems face in our ever-evolving world, CLAS ensures the demand for authoritative Information Assurance advice and guidance is met, to a recognised, consistent quality and standard.

It does this by creating a pool of expert consultants, approved by CESG, qualified to provide Information Assurance advice to government departments and other organisations that provide vital services to the United Kingdom.

Well done to everyone involved, and we look forward to offering even more specialised services moving forward.



Boxing Orange gains QSA status

The latest in our long list of professional accolades, Boxing Orange has recently been granted Qualified Security Assessor (QSA) status by the Payment Card Industry (PCI) Security Standards Council. As such we are now authorised to perform assessments of organisations that handle credit card data, measuring them against the high-level control objectives of the PCI Data Security Standard (PCI DSS).

The PCI QSA status is only awarded to individuals who meet specific Information Security education requirements, have taken the appropriate PCI training and are employees of an approved PCI QSA company. The certification also enables experienced security consultants to conduct the On-Site Data Security Assessment for PCI DSS Compliance.

Achieving QSA status means we can now offer even more specialist security services, including On-Site Data Security Assessments (PCI 'Audits'), Gap Analysis, Remediation Services and general PCI consultancy and advisory services.

This is great news for clients that are Level 1 Merchants or Level 1 and 2 Service Providers, as these require a QSA to conduct their annual On-Site Data Security Assessment and produce a Report On Compliance (ROC) for submission.

If you need help understanding which Merchant Level you are, which SAQ to complete, or for help on PCI DSS Compliance, call our in-house security experts on 0113 232 2330.

Forrester Report

In March 2010, independent technology and market research company Forrester Research Inc. published a report on the Managed Security Services Provider (MSSP) market. The report examined the growth and potential of the market and highlighted the reasons for this development over recent years.

It demonstrated how clients can use MSSPs to provide managed security services that may be impossible to deliver via internal resource. It also indicated that using an MSSP can significantly increase a client's security posture, knowledge and speed of remediation should an event occur. The report was compiled from a wealth of analyst experience, insight and research, through advisory and inquiry discussions with end users, vendors and regulators across industry sectors.

In the report, Boxing Orange is named as a World Wide Service Provider, and described as: "A UK MSS Provider that specialises in value-added service areas such as Security Information and Event Management". The report then goes on to name the top three industries as Government, Finance and Leisure & Entertainment.

We're thrilled to have been recognised in this way, particularly by such a respected industry specialist as Forrester Research, which has been providing its clients with pragmatic and forward-thinking advice about technology's impact on business and consumers for over 26 years. Uniquely, Forrester guides decision makers, marketing executives, business strategists, and IT professionals in creating unified technology plans that will help gain competitive advantage.

The report – "Market Overview: Managed Security Services" can be downloaded in full from www.forrester.com.

News



Richard Ackroyd

“More often than not, we find ourselves working with gaming companies to identify specific areas requiring attention, and delivering tailored services as appropriate, to fulfil individual business requirements.”

The betting industry has long been one of the most lucrative around, playing on the basic human desire to enjoy a quick win from a relatively small investment. With its origins in religious rituals and chance-based activities, gambling now worships at the altar of pure material gain. The odds, of course, favour the betting organiser, and today the betting industry accounts for billions of pounds, both over the counter and online.

Security Measures

Modern-day bookies have a number of ways in which they can conduct business, but invariably these all involve common payment and processing platforms containing data that requires securing. In the gaming industry, which is driven by the high-volume, low-value nature of betting, the most common concern by far is PCI Compliance.

Boxing Orange's range of managed security services, covering areas such as intrusion detection, file integrity, application and firewall, along with log management and event monitoring, address many points of the PCI Data Security Standard. But more often than not, we find ourselves working with gaming companies to identify specific areas requiring attention, and delivering tailored services as appropriate, to fulfil individual business requirements.

Data flows from consumers, whether via telebetting or online transactions, require pass-through-to-payment service providers. As a result of these rapidly increasing online revenues, credit and debit card details are being stored automatically to aid customers' online experiences, which means that both data transit and storage must be carefully addressed.

Website availability

Whilst the internet is the ideal way to deliver services to customers and generate business – who would complain about a shop front available to billions of potential customers? – the downside is that it is almost impossible to choose who is not welcome on the site.

In an increasing market sector that in 2008 was already reputed to be worth over £1.2 billion, there are already plenty of options for would-be customers to place bets. The most successful bookies will be those that offer online services with the best odds, that are easy to use,

respond the quickest and of course are readily available for both the traditional internet user and the new breed of mobile device clients. Speed, simplicity and security are key factors – the challenge is very firmly in the hands of the web and application developers, and those responsible for delivering maximum reliability to consumers.

The threat of Distributed Denial of Service (DDoS) has been around for the past 10 years, and whilst motives have changed during this time and the nature of the attacks themselves is constantly changing, the underlying desire to find weaknesses in web servers or infrastructure, that will cause major disruption, is definitely here to stay.

The consequences of downtime caused by DDoS attacks are severe: immediate loss of revenue in the short-term – which invariably is then handed to competitor sites – and the potential longer-term impact through permanent loss of customers to other competitors. Whilst the latter of the two outcomes is harder to put a tangible value on, forcing customers to use an alternative site in the short-term cannot be a positive step in revenue retention or growth.

What follows is an example that demonstrates the ways in which our managed security services have helped clients avoid these pitfalls.

**Global leaders in sports betting
William Hill case study**



William Hill PLC is universally recognised as one of the world's leading betting and gaming organisations. With over 70 years of bookmaking experience, the company serves many thousands of clients, and boasts the UK's largest retail betting estate of over 2,300 betting shops, a market-leading telephone betting service, and a successful betting website.

Since launching, William Hill Online has grown significantly, and the range of casino, poker and betting services offered firmly leads the strategy for continued growth in the online business sector. William Hill is quoted on the London Stock Exchange and is a FTSE 250 company.

In 2003, The William Hill Organisation chose Boxing Orange as their managed security services partner, and they've been a valued client ever since. Working closely with them over the years, we've built a strong relationship, and now assist them with all aspects of their IT Security. By providing managed services, consultancy and individual projects, Boxing Orange has ensured William Hill's PCI Compliance and improved their security posture.

“Security is crucial to the William Hill business; Boxing Orange's experience of the security threat landscape, DDoS, and the depth of technical expertise within the organisation is invaluable to William Hill. Our faith in the company has been borne out through our own experience and we are delighted to continue our partnership, which has grown over the past seven years.”

Alan Cook, Security Operations Manager, William Hill PLC



Richard Ackroyd looks at how Boxing Orange is enabling their major gaming clients to provide a safer arena for their valued online customers



Phillip Ineson

“ArcSight's SIEM Platform is used by the most demanding private and public organisations in the world.”



Above: Gartner Magic Quadrant for Security Information and Event Management (May 2010).

As many of you will be aware, ArcSight is one of Boxing Orange's key professional partners. They work closely with us to provide the tailored security solutions that our clients' businesses rely on every day. A global leader in their field, ArcSight's specialist knowledge and extensive implementation capabilities in the field of Security Information and Event Management (SIEM) mean we can always trust them to protect the platform that protects even the most sensitive of systems.

Why the ArcSight SIEM solution is top of the league

Boxing Orange have developed the ArcSight Security Information and Event Management (SIEM) Platform as a centralised enterprise security monitoring platform, designed to secure digital infrastructure, information, and business operations. It enables rapid identification, prioritisation, and response to policy breaches, cyber-security attacks and insider threats.

Currently, ArcSight's SIEM Platform is used by the most demanding private and public organisations in the world, so Boxing Orange is in great company. Organisations that have critical information, infrastructure or operations to protect, including the world's leading corporations in every major industry, governments worldwide, and the majority of intelligence, defence and civilian agencies.

ArcSight and the Gartner Magic Quadrant

The Gartner Magic Quadrant evaluates vendors based on their 'Completeness of Vision' and 'Ability to Execute', and positions them in one of the following quadrants: Leaders, Challengers, Visionaries or Niche Players. For several years, ArcSight has been identified by Gartner as sitting firmly in the Leaders Quadrant.

Following the recent publication of the 2010 Magic Quadrant for SIEM, ArcSight has been positioned in the top right of the Leaders Quadrant, demonstrating, once again, that they are ahead of the pack. Companies in this quadrant are acknowledged for offering functionality that is a good match to current customer requirements, as well as showing evidence of superior vision and execution for anticipated requirements. Leaders typically have relatively high market share and/or strong revenue growth, and demonstrate positive customer feedback for effective SIEM capabilities and related service and support.

An ever-evolving product range

At Boxing Orange, we're committed to rolling-out the ArcSight SIEM platform to all of our new and existing managed services customers, which we're currently in the middle of implementing. But thoughts are already turning to 'what next?'. ArcSight's expert product range and wide vendor support continues to grow, and Boxing Orange is keen to offer managed services around new and exciting products such as ArcSight Logger 4, ArcSight FraudView, ArcSight Express and ArcSight IdentityView. Over the next 12 months, our new Director of Security Services, Martin Dipper, will be working closely with ArcSight to deliver new and innovative security services to our existing and prospective clients. Ensuring we all stay at the forefront of specialist security management.



ArcSight Roundtable Event

Our Roundtable Security Events give industry and thought leaders in the field of information security the opportunity to hear a short and thought-provoking presentation on a hot topic of the day. Over dinner the topic is discussed at each roundtable before being opened to a discussion between the tables. So far, each of our three SIEM events has attracted the crème of the security industry from leading UK and global organisations. The next event is planned for Thursday 7th October 2010, where attendees will enjoy a presentation from guest speakers, ArcSight.

Meet our new ArcSight Account Manager

Boxing Orange is pleased to welcome Roy Duckles as our new ArcSight account manager. Roy has over 22 years' experience in IT, network sales, business application and sales management with major international IT vendors and systems integrators such as Cisco, Fortinet and Wipro.

The perfect platform
Why working with ArcSight means we never miss a thing



Martin Dipper

“The opportunities to replace older solutions are enticing for many companies, but the risk of moving sensitive data needs to be evaluated carefully.”

It's a term we have all probably heard at some point over the last 12 months, but what does it actually mean?

In brief, Cloud computing offers a way of handling IT requirements without the need for additional infrastructure, servers and in many cases, in-house IT specialists. As everything is hosted remotely and provided on demand, it can be a much more economical and scalable way of delivering IT services.

A good analogy would be to compare it with the establishment of the National Grid. Before this, companies often operated their own power stations, to generate and distribute the power they needed for their own individual use – a time-consuming and costly process. But once the Grid was established, everyone could access the power they needed from a central reserve, without having to physically stoke the fires themselves.

As a concept, Cloud computing isn't actually all that new – we have been using hosted services since the 90s, such as hosted email including both mailbox and hardware. What's new about the current services is the way they are delivered – over the wire, normally via a thin client such as a web browser.

“There are many benefits of opting for a Cloud-based solution, such as quicker and easier access of services, standardisation of service, and the cost efficiencies of flexible usage.”

Cloud computing can be broken into three distinct offerings:

Infrastructure as a Service (IaaS)

This is the ability for businesses to provision processing, storage and core computing resources, including operating systems and applications, in a hosted environment (“the Cloud”). The business doesn't manage the environment but does control the operating system, applications, and to some extent the networking options. IaaS is often delivered by hosting providers and is used to deliver web services and content for small and large organisations.

Platform as a Service (PaaS)

Here, businesses can provision applications using programming languages and tools in the hosted environment. The business doesn't manage the network, servers, and operating systems, but does have control over the applications and application hosting environment. This environment provides a platform that runs the application code on the provider's infrastructure, as in Google App Engine.

Software as a Service (SaaS)

Probably the most popular option, SaaS lets businesses use service provider applications running in a hosted environment. The applications are normally accessible using thin client and browser technology, via PDAs as an

example. The business doesn't control any part of the hosted environment, except maybe user-specific application settings. A good example of SaaS is salesforce.com.

There are many benefits of opting for a Cloud-based solution, such as quicker and easier access of services, standardisation of service, and the cost efficiencies of flexible usage. The launch of Google Apps and the pending launch of Microsoft Office 2010 (Web Apps) will allow more and more companies to move their office applications into the Cloud. The opportunities to replace older solutions with more interactive and readily-accessible services are enticing for many companies, but the risk of moving sensitive data needs to be evaluated carefully. The challenge now for security professionals and businesses is to understand the risks posed by the new services; not just those of confidentiality and availability, but also the regulatory and legal implications.

Serious about security

Security controls in the Cloud need to be reviewed in the same way as any IT environment. The risks need to be assessed and responsibility for physical security, operating systems, data and applications security have to be agreed and assigned. Cloud computing may be a newer model of control, but accountability for security still needs to be understood. As a business user, you need to know who can access your data, who has privileged access, how the Cloud provider vets and trains their staff, and what controls are in place to audit their access. You also need to ensure

that strong controls are in place to segregate your data from other customers. These controls should be inspected and tested by experts.

The nitty gritty – regulations and legality

The Cloud is ubiquitous and therefore your services could, in theory, be accessed from almost anywhere. Sounds great, but not always, as the recent case with Amazon has proved. Even though Amazon has no physical presence in North Carolina, they are being pursued for unpaid tax by the local tax authorities based on their sales in the area, and being pressed for a full list of their customers. This places Amazon in a hard place, as they either have to ignore the First Amendment and violate customer privacy, or face off the government tax collectors! Cloud services will create many more issues like this surrounding access to customer data and proprietary business information. In addition, hosting data in the Cloud still means your business is accountable for the security and integrity of its data, and your provider and the hosting process will need to be audited and maybe certified.

What if the worst happens? Business continuity and disaster recovery

“Where is my data hosted?” is a very good first question to ask your provider. Companies need a location with strong data protection and privacy laws. Commitments need to be agreed with the provider that they will obey data handling and privacy regulations in the region as they relate

to your business. Likewise, your hosting provider should be able to tell you what will happen to your data in the event of a business continuity event. Data needs to be replicated and recoverable in the event of the worst happening. Additionally, the long-term viability of the provider needs to be established early on. When negotiating the contract there should be a clear process in place for the return or transfer of your data to an alternate location.

Looking to the future

Will Cloud computing have a major impact on IT structure over the next five to ten years? Yes, for sure. Returning to the National Grid analogy, we are moving towards a solution where many users will operate from a ‘grid’ where the applications and services are customised and stored in the Cloud rather than locally. This makes sound sense – why does everyone need a full set of applications on their device?

As this approach evolves, businesses will need to work with strong local providers to review the security and operational aspects of this approach. At Boxing Orange, we are already delivering a range of services that will operate in a Cloud- or premises-based scenario, detecting threats across your business wherever the data and the users are situated. Rest assured, we are already considering the future of an application-driven security world, and developing innovative services that will support our customers today and into the future.

Taking our heads out of the clouds

Martin Dipper encourages us to plant our feet firmly on the ground and get to grips with Cloud computing



Events

Throughout the year, we run a range of industry-leading events, from joint educational seminars with our partners, to attending security and IT exhibitions. Over the next few months, we'll be hosting a number of roundtable discussions – see below for more information and details on how to book your place.



Data Loss Prevention Roundtable Event

Many organisations are unknowingly failing to meet government and commercial regulations that mandate controls over how information is stored and processed. The loss of large volumes of protected information has become a regular headline event, forcing companies to re-issue cards, notify customers, and mitigate loss of goodwill from negative publicity. In order to stop the loss of sensitive information, many organisations are turning to Data Loss Prevention services and technologies. Boxing Orange will be holding a roundtable discussion on Data Loss Prevention, highlighting the ways in which data can be lost, how to prevent data loss, and the importance of understanding where critical data is held.

When Wed 6th October 2010
Where Ritz Hotel, London

SIEM Roundtable Event

After a year of successful Security Information Event Management roundtable events, Boxing Orange is once again delighted to host a further SIEM roundtable discussion at the Ritz Hotel, London. As with previous events, a diverse range of Security professionals from all vertical sectors will be attending. Previous guests have included some of the UK's largest end users, including British Airways, J.P. Morgan Asset Management, Sony and Tesco.

When Thurs 7th October 2010
Where Ritz Hotel, London
Guest speaker ArcSight

Please note that places are limited for both events, so to reserve or for more information visit www.boxingorange.com, call **0113 232 2330** or email marketing@boxingorange.com