DATA INTEGRATION | WHITEPAPER

CONNECT TO EVERYONE, TRUST NO ONE

Data Integration for Cyber Attack and Threat Mitigation solutions.

DATA INTEGRATION
An Xchanging Company

Your Cyber Defences Will Be Breached.

Overview

Security analysts, including the Ponemon Institute, consistently report that data breaches are becoming more frequent and more severe. Most industry commentators agree that it is not a case of if a business will suffer data breaches, but simply when. It is only a matter of time.

Breaches can be malicious or non-malicious, but whatever the intent, any theft of business data, operational disruption or the 'brand impact' can be extremely costly. We should be setting up our networks and defences to treat all disruptive traffic as malicious, and then mitigate it accordingly. Just because a Denial of Service (DoS) attack was the result of a misconfigured server and not anonymous, won't make it any less of an attack – your service is still denied.

The cost of a breach is measured by the value of the data released, resources spent detecting and responding to the attack, regulatory fines and decreased revenues from loss of business reputation.

The cost of a breach is measured by the value of the data released, resources spent detecting and responding to the attack, regulatory fines and decreased revenues from loss of business reputation. When Adobe suffered a theft of data from an external source in October of 2013, impacting over 125 million user accounts in the wild and counting, the ongoing press coverage has potentially caused serious, deep rooted harm to the organisation and its brand; not to mention what was actually taken - the source code. The implications of this are huge and largely unknown as of now, but we can imagine what this could mean: free reign to crackers over Adobe's software authentication, allowing piracy to surge and revenue to tumble. Additionally, they could reverse engineer patented technologies – a freeware PDF editor would hurt sales of Acrobat. Perhaps the most important question, what else did they take or amend whilst they were in there, unsupervised? Similar to the NSA/ Snowden revelations, how will they know when it's over?

Accept you will be attacked

If you accept that your business will suffer from a successful cyber-attack then the key question to ask yourself is: How can I minimise the impact of a breach and what strategy should I implement to achieve this?

It's important to remember that even partially successful attacks need to be identified and mitigated regularly and methodically. Hackers use tools and scripts which are readily available many used by the "white hats" and security researchers to probe for potential weaknesses in your defences. They then log the results as "interesting" if not yet vulnerable for selling on, depending on how important the data is, and how attractive it may be to attackers. For example, a firewall interface responds but rejects a connection, rather than simply not responding; this is an event of interest to a hacker as it tells them something is there, just not yet accessible. Automatic tools collect hundreds of thousands of these events each day, which are searched, collated and data mined with such efficiency that would make many enterprises envious. This is the modern version of what used to be called "war dialing". In the days of modems you would dial a number, see if it's a modem, dial another, and another – ad infinitum. It's a bit faster than that now, but these bad guys are smart people.

The key here is that "war dialing", or probing, is as useful to you as it is to the attacker – provided it's noticed and analysed. This is how technical honey traps lure attackers. But what if the attack isn't targeted at your honey trap? What if the attacker isn't fooled, which is more than likely in this hacking era, what if the mere fact that you have a honey trap piques the interest of an attacker?

We need to use devices and software which are dedicated in looking for these ripples in the water; they indicate there may have been something there seconds previously.

The solution

Our Cyber-Attack and Threat Mitigation portfolio is an integrated solution platform focused on addressing the post-breach issues businesses face following a successful cyber-attack.

It will identify, contain, respond, remediate and ultimately mitigate the impact of the breach, faster and more efficiently than ever before. It helps address the key issues facing CISOs: lack of visibility, volume of incidents, classification of incidents, time to detect, time to contain and ultimately the minimisation of the attack's impact.

With this solution, a business has superior intelligence and visibility into the ICT infrastructure and faster notification of any breach. Consequently they will be able to remediate more quickly and ultimately minimise the cost to the business, downgrading successful attacks to defensible threats.

Crucially, our collection of tools, vendors, software, expertise and managed services allows us to constantly learn about the attackers and the profiles of their attacks.

It shouldn't be forgotten that although the vast majority of attacks are opportunistic and the result of a scattergun "hit and hope" script running from Metasploit / Armitage or a Backtrack host, are therefore normally (not always) recognisable and dealt with by robust security systems. However, there is another type of attack, used by an altogether different type blackhat – the targeted attack.

A targeted attack

As implied by the name, there is always a reason behind a targeted attack, and the victim must always do all they can to understand what that reason is. It may well not affect their policy or business decisions in the future, but at least they will be aware that certain actions often result in an increased threat level. Think of the number of corporate and customer facing websites which have been targeted and taken out of service (sometimes for prolonged periods of time) because the actions of the parent company or governing body have offended hacker collectives in some way – Visa, Mastercard, Bank of America, Greenpeace, The United Nations, chemical and drugs companies, local and national government – the list is extensive.

Businesses may suddenly be getting websites and ISP bandwidth swamped with sessions originating largely from a certain country, city or continent. Think about business communications and news; has your business recently announced major gas fracking operations in that region? It sounds simple, but this level of intelligence is crucial to understand both current risks and those associated with future activities.

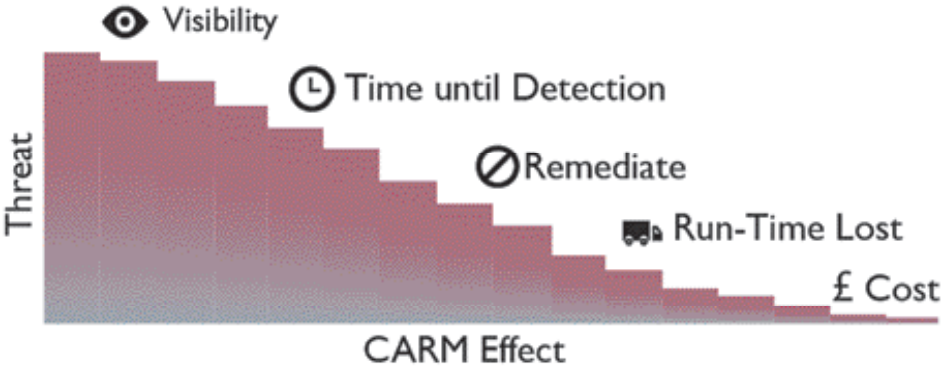
With Data Integration's Cyber Attack and Threat Mitigation solution, a business has superior intelligence and visibility into the ICT infrastructure and faster notification of any breach.

Think about how your business compares to your peers. If you make chocolate eggs, have you sustained more or less of an attack than the other chocolate egg manufacturers? How about the chocolate industry in your country? Or confectionary conglomerates worldwide? How does it compare to last week or last year? This is crucial information for an IT security department to have and for an ISO or CISO to take to the board and explain the level of threat and security pertinent to their business. This can all link to budgetary and investment decisions, team sizing, technical strategy and myriad other things.

Targeted attacks are dangerous, difficult to defend against, well researched and often reliant on pretty simple user manipulation via a combination of social engineering and technical skill.

Your users are the new attack vector. It's so much simpler to trick someone in your organisation into clicking on a link or opening an image, than it is to spend hours and days scanning for vulnerabilities, picking away at a firewall hole hoping it doesn't notice. It's not the user's fault. Users are savvier than ever, have more training than ever and are more aware of the risks than ever. But they're also more connected than ever, at home, on the move and at the office. Car accidents were pretty rare when there were only 1000 in the world.

The commissioned hacker knows their target – it's easy - they go after the Financial Director on LinkedIn and simply find an email through social media or websites.



The hacker now knows the contact and it's easy enough to send an appealing embedded link, then use an unauthenticated SMTP server to send an email with the "from" field amended to reflect that of your FD's best friend and they're in. The link doesn't seem to work – your FD may or may not follow it up, chances are not – but what they just did was open a port to a malicious webserver which has reconfigured their browser for use as a proxy, capturing everything they do through the web. Or perhaps it could run some tests to see what level of code can be executed within that browser by Java without attracting attention, which could then allow a tiny remote control application or keylogger to be installed. Within minutes that machine, with the logon credentials, is compromised, and that commercially sensitive data is sitting in a Dropbox folder waiting for your competitor to collect it.

A university research study in the US discovered that the people most likely to click on links and respond to well-crafted phishing attacks were executives and those working in IT security. The IT security group was puzzling at first – but it seems to be a straightforward case of complacency. People very often do not follow their own advice, and with a detailed knowledge of the risks may feel a kind of immunity over time. It's also why motorcyclists wearing leathers ride faster – it feels safer, but it's most certainly not.

A university research study in the US discovered that the people most likely to click on links and respond to well-crafted phishing attacks were executives and those working in IT security.

In summary – security is not about equipment, knowledge or skilled ISO and IT teams. It's not about user education, intrusion detection, certifications, audit requirements or policies and procedures. It's not about firewalls, market awareness, research, monitoring or reporting. It's not about users, induction courses or joiners and leaver's policy. It's about all of this and more, working in unison.

Why do you need this?

Breaches are a global occurrence. According to Verizon, there were 47,000 known security breaches in the USA in 2012, whilst in the UK, PWC has reported that every large (>250 employee) business suffered an average of more than 54 attacks throughout that year. The average cost of a data leak is anything up to $5.5m.

These few statistics rely on reported and survey data so are only the tip of the iceberg. How many incidents went unreported, how many breaches weren't found, how many businesses kept their problems a secret?

The bottom line is that breaches happen and when they do they cost a lot of money; this solution will help you minimise that cost.

The steady growth of a 'big security' problem

The opportunities for malicious cyber activity are increasing.

- The number of devices on a corporate ICT infrastructure continues to grow; many employees now access business information from two or more devices rather than just a PC.
- BYOD is leading to a proliferation of devices that cannot be rigorously controlled by the IT department; system and antivirus software might not be up to date.
- Cloud services are providing malicious perpetrators both with new points of entry and the computational resources to power their attacks.
- The success of the Android OS is acting as a magnet for malware; all security vendors are reporting a massive increase in the number of threats propagating throughout the Android ecosystem.
- App stores are adding to the complexity of the security problem; the triumvirate formed with BYOD and mobility has opened the door to a range of 'unapproved' applications that employees are using to improve their productivity.

The magnitude of cyber security threats is increasing in line with the available attack surface. According to a Ponemon Institute global survey of 3,500 IT security practitioners, over 50% reported an increase in the frequency and severity of cyber-attacks on their organisations during 2012.

Cyber Threats: Origination

Current evidence leads security experts to broadly agree that around 75% of data breaches originate from outsiders, whilst less than 10% come as a result of a malicious insider.

Verizon figures show that 76% of incidents are initiated via a network intrusion made possible by weak or stolen credentials. Although there were fewer incidents involving the combination of malware and hacking, this remains a major means of attack. Significant growth in social engineering mechanisms has also been tracked throughout 2012, particularly phishing.

Personal information, and in particular cardholder details, accounted for over 95% of exposed data according to a report by Trustwave.

Cyber Threats: Sophistication

Cyber threats are growing in sophistication and are consequently much more difficult to deal with.

Combinations of all the well-known techniques including trojans, phishing, hacking, botnets and SQL injections are being cleverly constructed into long term initiatives by well-organised bodies including government funded agencies and criminal entities alike. Collectively known as Advanced Persistent Threats (APTs), they represent a far greater risk and far greater detection challenge than traditional means.

Often included within an APT, is the so called 'Zero Day', which exploits a new approach to the process of cyber-attack detection. By definition there is no precedent for them, hence there is no previous reference signature that defence systems can refer to.

And whilst traditional malware continues to evolve; new forms of polymorphic threats are emerging which, as the name suggests, are able to change more dynamically and adopt a variety of disguises.

Cyber Threats: Commoditisation

Cyber threats are leveraging the advances in computing which continue to march in time to 'Moore's Law'. It is no surprise therefore that capabilities and threats which were once the domain of national governments and agencies, are now within the reach of the criminal fraternity.

The development of very sophisticated cyber security threats is now perfectly achievable by individuals of the appropriate persuasion and skill. The growth of developer communities feeding the App Store ecosystems has fuelled this commoditisation.

Why is it still a problem?

Post breach boom!

Businesses are finding that, despite the system investments, policies and procedures, they continue to be breached and continue to be challenged to remediate and mitigate the impact.

Moreover, breaches in corporate infrastructure are often only spotted hundreds of days after the initial penetration (research suggests circa 400 days); by which time, target credentials and data have long since gone.

Impact Summary

So your ICT infrastructure has been breached, and you've lost some data. Is it really such a problem?

The impact of a breach on a business can be hugely significant. The costs may be truly massive. There is the direct cost of addressing the breach by pulling people and resources away from other work to investigate, forensically analyse and identify the source of the breach, and then determine a response and remediate existing systems. However, these substantial costs can be small in comparison to those incurred through damage to the brand by customers churning, investors selling or competitors gaining intellectual property.

The basic issue: BIG Security

Fundamentally, CISOs are struggling to combat a BIG security problem!

Cyber-attacks are becoming more frequent, more severe (expensive) and harder to detect. There are insufficiently skilled people available in the business to address the issues and there's no one to clear up after a successful attack.

Put another way, current ICT infrastructures don't provide sufficient visibility to detect anomalies or other indicators of change. The volume of attacks is producing a BIG data problem. These issues are delaying the identification, classification and qualification of the most dangerous attacks. Formulating a response is taking too long and insufficient resources are delaying the appropriate remediation. Little effort is left to complete a forensic study, develop the regulatory or compliance reports and managed mitigation is a pipe dream.

So what is needed?

A new approach is required to address these issues. The business needs an early warning system for an impending attack, or at least a fast alert of a successful breach, together with a combination of defensive systems that can be rapidly re-configured to stop the attack.

To manage this and provide a holistic view, a centralised command and control capability is needed which can interrogate devices, systems and applications throughout the infrastructure in order to detect and locate the point of entry, then disable or block it immediately. A platform that provides you with all-round visibility on the network, giving you insights you've not previously had.

Introducing Data Integration

Data Integration's network solution automates cyber-attack's threat and mitigation. We can help a business answer the who, what, why, when, where and how of an attack so that it can formulate a suitable response to remediate and mitigate the impact.

Cyber-Attack and Threat Mitigation Attributes

We implement and manage a process which links a business's ICT defensive capabilities to its cyber-attack identification systems and its response development procedures, then rapidly instigates the remediation of the defences – all in an automatic or semi-automatic fashion.

The solution detects signature-less threats such as Zero Day attacks and correlates event logs from across the complete ICT infrastructure to reveal, qualify and isolate attacks. It then creates and delivers appropriate reconfigurations to the defensive systems as a remediation to block and stop the attack dead in its tracks.

It provides inside-out (as well as the more traditional outside–in) protection. This is critical in cases such as those involving sinister APTs which often lie undetected, yet continue to shift key data out of the network. It also identifies the export of all data and can correlate it against corporate policies and user profiles, and will in most cases catch such illegal transfers.

Finally, we deliver real-time monitoring, BIG data analysis with anomaly detection, fast incident identification and classification, quick response formulation, reconfigurable defences, security control, reporting to automatically deliver the process of defence, identification, isolation, and response and remediation.

Building a Cyber-Attack and Threat Mitigation Solution

This platform offers businesses the opportunity to establish a customised solution to meet their security needs; an extensive portfolio of state of the art security vendor products which provide overlapping capabilities across the four functional areas of the solution: Defence, Identify, Response and Remediation.

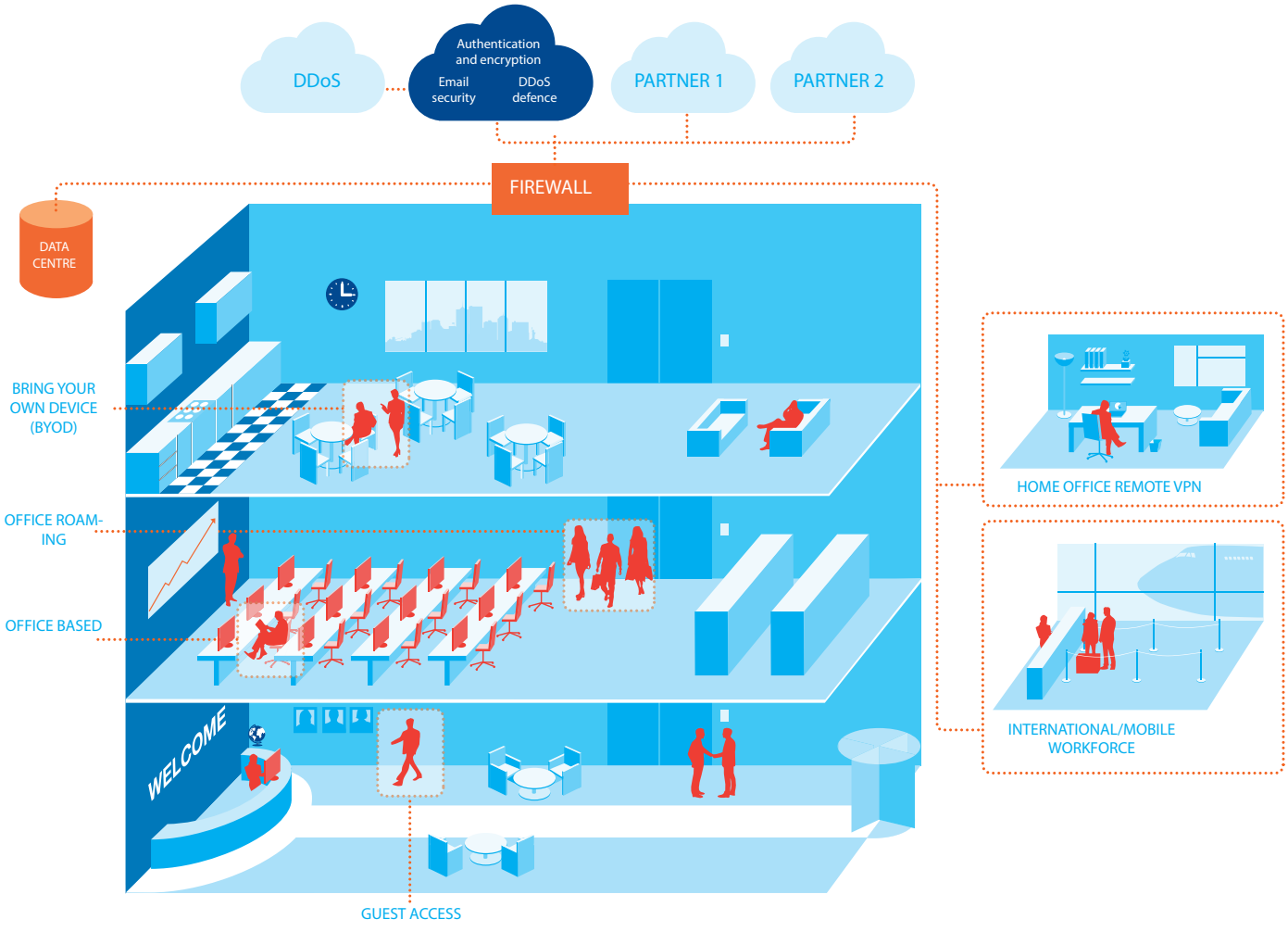
Depending on the investments the security department has already made, this solution can be crafted from the portfolio which will incorporate the legacy security infrastructure. It's not a rip and replace but rather leverages previous investments which were designed for prevention purposes to deliver a post-breach solution.

Benefits

The post-breach scenario is an extremely big issue for CISOs. Many are struggling to minimise the cost to their business. Typically their investments to date have been aimed at protection, but with overwhelming evidence to suggest breaches are becoming more frequent and severe they now need to turn their attention to building capabilities to shorten both the time to detect a breach and the time to contain it. Time is money, the longer a breach remains open, the more it will cost the business.

In the face of an increasingly hostile cyber environment, businesses need to come to terms with the very high probability that they will suffer a successful attack, that their defences will be breached, and that important data records will be stolen. It's time for investors to recognise this and allocate resources to minimise the impact.

What does it look like?



Contact us today to
discuss your
Cyber Defences.

Xchanging UK
34 Leadenhall Street,
London, EC3A 1AX, UK
+44 (0)20 7780 6999
www.xchanging.com