The odds are against you! Protect your business data with CARM

Whitepaper
Your cyber defences will be breached!

Security analysts, including 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 as a result of cyber attack, but simply when. It is only a matter of time.

Breaches can be malicious or non-malicious but whatever the intent, any exposure or theft of business data, operational disruption or the ‘brand impact’ is extremely costly. The cost of a breach is measured in terms of the value of the data released, the resources spent detecting and responding to the successful attack, regulatory fines and decreased sales revenues owing to loss of business reputation.

If you accept your business will suffer from a successful cyber attack then the key question to ask yourself is: how to minimise the impact of the breach, and what strategy you will implement to achieve that.

Exclusive Networks offers you CARM: Cyber Attack Remediation & Mitigation.

What is CARM?

CARM is an integrated solution platform focused on addressing the post-breach issues businesses face following a successful cyber attack.

The CARM platform allows you to identify, contain, respond, remediate and ultimately mitigate the impact of the breach, faster and more efficiently than ever before.

By combining the best of breed capabilities of a number of vendors, Exclusive Networks is able to demonstrate how CARM will help 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 CARM, a business has superior intelligence and visibility into their 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.

CARM downgrades successful attacks to defensible threats.

Why do you need CARM?

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 £3.5m.

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; CARM helps 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.

Again using Verizon figures, 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 know 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 threats.

Often included within an APT, so called ‘Zero Day’ exploits demand 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 that, 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.
Post breach boom!

Businesses are finding that, despite the system investments, policies and procedures that they have invested in to prevent successful cyber attacks, 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, as noted above, may be truly massive, coming as they do both directly and indirectly. 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. 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 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 attack point of entry and 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 CARM

Exclusive Networks’ CARM platform offers to automate Cyber Attack Remediation and Mitigation.

CARM helps a business answer the ‘Who, What, Why, When, Where & How’ of an attack so that it can formulate a suitable response to remediate and mitigate the impact.

By implementing a process of defence, identification, response and remediation, CARM downgrades successful attacks into known threats.
CARM attributes
The CARM platform implements a process which links a business’s ICT defensive capabilities to its cyber attack identification capabilities and its response development capabilities, and rapidly instigates the remediation of the defences – all in an automatic or semi-automatic fashion.

CARM 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.

CARM 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 in a quiet backwater of the ICT infrastructure yet continue to shift key data out of the network. CARM 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, CARM delivers real-time monitoring, BIG data analysis with anomaly detection, fast incident identification and classification, quick response formulation, reconfigurable defences, security control, and reporting to automatically deliver the process of defence, identification, isolation, response and remediation.

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

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

Instilling CARM
Exclusive Networks can demonstrate a selection of configurations of the CARM integrated platform using the appropriate blend of technology from leading vendors such as LogRhythm, FireEye, Palo Alto Networks, Bit9, Imperva, Mandiant and Fortinet.

Exclusive Networks can simulate a wide variety of attack vectors and demonstrate how CARM rapidly isolates and remediates a breach.

CARM reverses the trend of escalating threat

<table>
<thead>
<tr>
<th>Trend since 2012</th>
<th>Large organisations (&gt;250 staff)</th>
<th>Small businesses (&lt;50 staff)</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of respondents that had a breach</td>
<td>⇆</td>
<td>↑</td>
</tr>
<tr>
<td>Average number of breaches in the year</td>
<td>↑</td>
<td>↑</td>
</tr>
<tr>
<td>Cost of worst breach of the year</td>
<td>↑↑</td>
<td>↑↑</td>
</tr>
<tr>
<td>Overall cost of security breaches</td>
<td>↑↑↑↑</td>
<td>↑↑↑↑↑</td>
</tr>
</tbody>
</table>

Source – PWC 2013
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 investments to recognise this and resources allocated to minimise the impact.
CARM benefits

The post-breach scenario is an extremely big issue for CISOs. Many are struggling to minimise the cost to their business of a security breach. 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.

Summary

Like it or not, the IT industry is now in the midst of a post-breach era. Businesses will be breached. They need to develop an economic way to address the issue.

CARM is the platform that will help them achieve that goal. CARM simplifies and automates the processes involved in detecting, identifying, qualifying and responding to a breach.

CARM is a real-life working platform available and demonstrable today. Call your Exclusive Networks account manager or active reseller to book a demonstration.