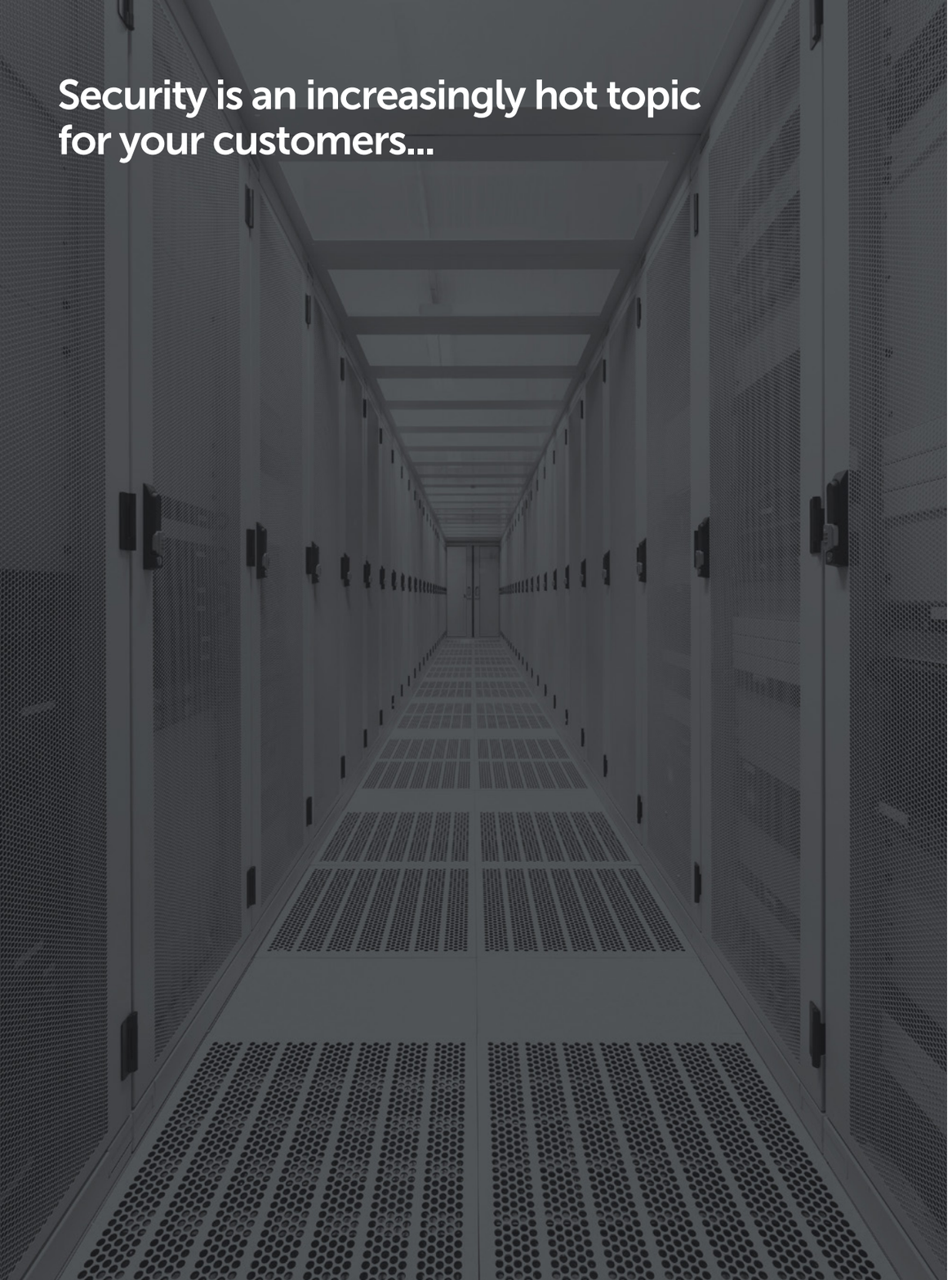
inbay

FROM AWARENESS TO ACTION

MOVING BDR UP YOUR CUSTOMERS' PRIORITY LIST



Security is an increasingly hot topic for your customers...

...but how can you turn this growing opportunity into lasting revenue for your business?

One theme coming through very strongly in recent security research findings is that it is not just big companies who need to have effective security and backup and disaster recovery (BDR) policies in place. Today, businesses of all sizes are at risk from data loss resulting increasingly from cyber-attacks such as CryptoLocker-type ransomware.

Ransomware cost companies 325 million US dollars in damages worldwide in 2015 alone.[1]

The last five years have seen a steady increase in attacks targeting businesses with less than 250 employees, with 43 percent of all attacks targeted at small businesses in 2015, according to the latest Internet Security Threat Report (ISTR) from Symantec[2].

Small-medium sized businesses (SMBs) may be more likely to suffer a cyber-attack because their IT team may be at best stretched too thin – and at worst non-existent. This is why many are looking to their managed service providers (MSPs) for specialist help.

Add to this lack of in-house resource and specialist knowledge a level of budgetary constraint that is forcing a dependency on outdated technology and you have the ideal conditions for ransomware vulnerability.

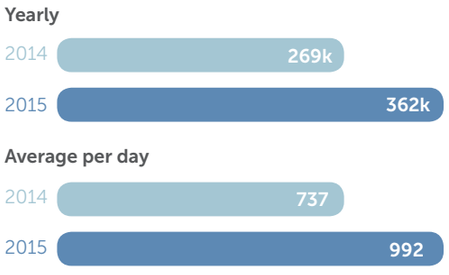
These SMBs may include your customers and prospects.

So, if you haven't already had the BDR discussion with them – now is a very good time to do it. As well as making them more aware of the potential risks they face, this dialogue could open up a whole new area of service opportunity for your business – and cement your role as trusted adviser.

[1] Cyber Threat Alliance: Lucrative Ransomware Attacks, 2015
[2] Symantec, Internet Security Threat Report (ISTR), April 2016

Ransomware: weapon of choice of today's digital highwaymen

Number of crypto-ransomware incidents



Source: Symantec's Internet Security Threat Report

Ransomware has existed for almost 20 years, but it became the 'weapon of choice' in 2013 with the emergence of CryptoLocker. By the time the original CryptoLocker botnet was shut down in May 2014, the cyber criminals behind it had extorted nearly three million US dollars from victims[3].

Since then, variants on the CryptoLocker theme have appeared and continue to evolve: CryptoWall, CTB Locker, Locky, TeslaCrypt and TorrentLocker to mention some of those more commonly found today.

How is ransomware distributed?

Spam, Spam, Spam, Spam[4]

Ransomware is distributed in many different ways – most frequently via ever more convincing spam, with victims tricked into downloading a rogue email attachment or clicking a link. Once the victim downloads or clicks, the malware is installed on the system and begins to encrypt files.

Exploit kits

Also known as a 'drive-by download', this kind of attack isn't necessarily initiated by a victim's action. The exploit kit has been designed to identify system vulnerabilities and exploit them to enable ransomware to be installed. In this type of attack, hackers install code on a legitimate website that redirects computer users to a malicious site.

There are various exploit kits in use, but 'Angler' is the one most commonly encountered today. It uses HTML and JavaScript to identify the victim's browser and installed plugins, allowing the cyber-criminal to select the attack that is most likely to be successful. Angler is constantly evolving to avoid detection by security software products, making it difficult to protect against.

Ransomware-as-a-Service (RaaS)

RaaS is a kind of 'affiliate distribution' scheme for ransomware that can be signed up to on the 'dark web' – and worryingly, requires little by way of technical expertise to exploit it, hence widening the pool of potential cyber criminals.

[3] Datto – The Business Guide to Ransomware
[4] www.youtube.com/watch?v=mBcY3W5WgNU

Front page news – spreading the fear

66%
of small businesses have been a victim of cyber crime

Cyber crime costs each small business victim nearly
£3,000

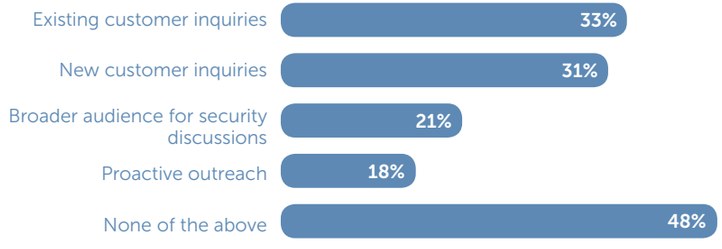
four in two years
On average a small business is a victim of four cyber crimes every two years

Source: The Federation of Small Businesses (FSB) UK: Cyber Resilience: How to protect small firms in the digital economy, June 2016

Security breaches in general and ransomware incidents in particular make front page news these days – particularly when they affect major corporations or government agencies. CompTIA[5] refers to the 'ripple effects' that such headlines have on enquiries to channel firms about security services, as shown in the table below.

Your customers and prospects will undoubtedly already be aware of the bigger cyber-attacks from the media. What they may be less familiar with is the extent to which cyber-attacks are increasingly hitting small-medium sized businesses.

Ripple Effects from Security Breach Headlines



Source: CompTia, Trends in IT Security, March 2015

[5] CompTia, Trends in IT Security, March 2015

What makes SMBs particularly vulnerable?

Not following effective cyber-security practices is probably the main reason, combined with human error and the almost irresistible tendency to open attachments or click on links that are becoming ever more convincing.

Eight common areas of vulnerability

1. Lack of knowledge
2. Lack of awareness of full implications of a cyber-attack
3. Limited resources (time, expertise and budget) to implement comprehensive security defences
4. No dedicated IT security specialist in-house
5. Inadequate employee security training
6. Failure to secure endpoints
7. Outdated systems and failure to invest in new technologies that would help to keep them secure
8. Outsourcing security to generalist contractors, rather than specialists

Exploiting SMB vulnerability

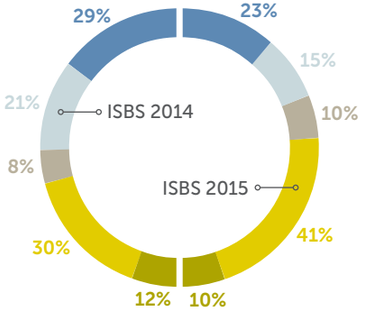
SMBs can no longer assume that they are too insignificant to attract the attention of cyber criminals.

And it is not just a question of their businesses being at risk.

Increasingly, cyber-engineered attacks on SMBs are designed to open the door to systems further up the supply chain – those of enterprise-level companies and government entities, in particular. Today's SMBs are increasingly 'digitally entwined' to the bigger companies they are working with - and as such may have trusted access to the networks and data of these customers and partners.

Thus a failure to protect effectively against cyber-attacks could put the SMB's entire reputation at risk. Indeed, a recent PwC survey[6] found that among the drivers for information security expenditure, 'protecting customer information' and 'protecting the organisation's reputation' account for over half of the responses.

The reputational impact of a breach



- Business disruption
- Cost to investigate and fix
- Value of lost assets
- Reputational damage
- Other

Source: 2015 Information Security Breaches Survey, PwC/InfoSecurity Europe

"When asked what made a particular incident 'the worst', 16 out of the 39 organisations who responded cited that it was the damage to their reputation which had the greatest impact. This is an increasing trend, up from 30% of respondents in 2014 to 41% this year."

[6] 2015 Information Security Breaches Survey, PwC/InfoSecurity Europe

But every cloud has a silver lining

Because where there is a threat, there is nearly always an opportunity – and in this case, BDR/business continuity for SMBs represents a huge opportunity for MSPs.

BDR/business continuity is a real growth area, expected to increase from US $5.2 billion in 2014 to US $7 billion in 2019[7].

Within this, the fastest growing segment is predicted to be Disaster Recovery as a Service (DRaaS). This market is expected to be worth US $11.92 billion in 2020, from a base of US $1.42 billion in 2015[8].

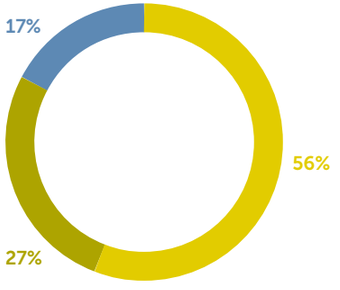
And the findings of a CompTIA survey[9] of 400 US companies found that MSPs were "particularly positive" about the potential growth in security revenue moving forward.

Many already offer a range of managed IT services and see security as a logical extension. Nearly 3 in 5 channel firms incorporate security services in some form already, as shown in the chart below.

At the very least, CompTIA concludes, MSPs must begin by demonstrating greater awareness of the security landscape and by highlighting any mistakes being made by their customers. They may then begin to introduce additional security services.

The difficulty lies in engaging your SMB customers in a first serious business continuity discussion – then moving it further up the priorities list.

Security Offerings from IT Companies



- Standalone product/service
- Embedded in other product/services
- Not offered

Source: CompTIA, Trends in IT Security, March 2015

Types of Security Offerings

57% Network security
56% BC/DR
51% Data protection
48% Email/Web security
42% Compliance management
42% Risk management
42% Cloud security
38% Identity access management (IAM)
37% Intrusion detection
35% Mobile security
33% Security information and event management (SIEM)

[7] Gartner, quoted in BusinessWire, January 13, 2016
[8] MarketsandMarkets Research
[9] CompTia Trends in IT Security, March 2015

Five hooks to get the BDR ball rolling with your customers

1. Move the discussion beyond 'backup' to focus on the disaster recovery/business continuity aspect of BDR.
2. Focus on speed of recovery: your customers may not be taking account of the length of time needed to recover from a disaster using traditional backup technology. If this is days or even weeks, then they will suffer serious disruption to their business – as will their customers.
3. Focus on the cost of downtime to the business as a result of a cyber-attack or security breach.
4. Emphasise the reputational cost if their systems are used as a Trojan horse to smuggle malware into their customers' systems – as well as the loss of confidence among all their other customers resulting from business disruption while the cyber-attack is being resolved.
5. Focus on the skills shortage that is making it more difficult for SMBs to identify and prevent cyber-crime – and how partnering with the right MSP can provide ready access to these skills.

Moving disaster recovery beyond backup

Ransomware 'punishes' businesses that don't have a robust BDR strategy in place. Most SMBs know the importance of regular backups – but ticking the 'backup' box is not in itself enough.

Your customers may have purchased cloud storage and believe that this is an adequate backup solution.

Speed of recovery

What they don't always factor into the equation is the length of time needed to recover from a disaster using traditional backup technology – or the impact that this potentially very long period of downtime may have on their business. Restoring data from off-site tape or traditional cloud backups can be painfully slow – and access to replacement systems and networks may also be needed to restore the data.

So any discussions with customers about disaster recovery/business continuity planning need to begin with an assessment of the amount of downtime their business could tolerate, focussing on two aspects in particular:

- Recovery time objective (RTO), i.e., how quickly data must be recovered;
- Recovery point objective (RPO), i.e., which data needs to be recovered and from when (usually a date-based parameter, e.g. forward from six months ago).

Cost of downtime

Downtime equals lost time.

All unplanned downtime has a cost as a result of:

- Lost revenue
- Lost productivity
- Direct recovery costs
- Reputational cost

It can be useful to demonstrate to your customers and prospects the true cost of losing access to their systems for a period of time – and how the price of additional security services can be offset against this potentially much greater cost.

It is relatively easy to do at a high level: take account of the number of employees who would be affected, their salaries and overhead costs – and add in the estimated revenue lost by each for each hour of downtime.

Indeed some business continuity specialists offer a calculator that will help you to work out the total cost of downtime.

They may be very surprised to learn what the total cost of downtime would be.

Indicative financial impact of downtime on the business

- **552** employee work-hours are lost annually when IT systems fail and employees cannot access their files; this represents more than a quarter of the year for a single employee of a typical small business.
- **$20,000** is the average hourly loss through downtime as a result of the disruption.
- **$75,000** is the hourly loss if the disruption extends to three hours and employees cannot get back online and resume work.

Source: Datto: 5 Keys to Creating a Disaster Recovery Plan for SMBs, 4 February 2016

Reputational cost: the biggest price to pay?

Quite apart from the risk of being used as a conduit to their customers' systems, the disruption to business caused by cyber-attacks can cause severe reputational damage and loss of business.

KPMG's report on 'Small Business Reputation and the Cyber Risk'[10] sets out these risks clearly and is a great marketing aid to put in front of your SMB customers and prospects.

Several extracts are included here.

The impact of a cyber-breach - 'huge and long-lasting'

The survey concluded that of the 599 small businesses that experienced a cyber-breach, the majority (89%) felt the attack impacted their reputation. Even so, they may be underestimating the extent of this impact: 58% of the consumers surveyed said that a breach would discourage them from using a business in the future; while a further KPMG Supply Chain study revealed that 86% of procurement departments would consider removing a supplier from their roster following a cyber-breach.

For small businesses who have experienced a breach, the impact has been long-lasting, with more than one in four (26%) unable to grow in line with previous expectations, and almost a third (31%) saying that it took over six months for the business to get back on track.

Quality of service is also at risk

Those who experienced a cyber-breach found that it caused customer delays (26%) and impacted the business's ability to operate (93%).

The report cites an average of 26 hours [needed] to resolve a breach by small businesses, which, as KPMG points out "is a large chunk of time to stop running your company to deal with an issue – not to mention the costs incurred and it being all too obvious to your customers."

89%
Of the small businesses surveyed who have experienced a breach said it impacted on their reputation. Those who experienced a breach said the attack led to:

31%
Brand damage

30%
Loss of clients

29%
Ability to win new business

Quality of service is also a risk:

26%
of those surveyed who experienced a cyber breach found it caused customer delays

93%
found it impacted the business' ability to operate

[10] https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

Why you should be positioning the benefits of outsourcing BDR/business continuity

Forewarned is forearmed when it comes to pre-empting and combating cyber-attacks effectively.

The most common reasons cited by SMBs for an absence of BDR/business continuity planning are a 'lack of knowledge, lack of time and lack of resources' to prepare effectively.

Outsourcing to an MSP who has the specialist skills required and dedicated BDR/business continuity resources can help to plug these gaps.

You can overcome your customer's 'lack of knowledge' with a gradual education process – which will also strengthen your role as trusted adviser.

You can supplement their 'lack of resources' by providing support from your own team of qualified technicians.

And, recognising the perception among SMBs that a BDR/business continuity solution will demand a lot of management time, including the time required for setup, testing and ongoing maintenance – you can help by taking on some or all of this routine management responsibility.

But of course you need to be sure you can successfully deliver BDR services alongside your existing offering.

Partnering can help you to deliver BDR/ business continuity services

BDR is a specialist area and as an MSP your choice of partner needs careful thought.

Partnering with the right business continuity specialist for your business can give you access to the latest technology products and the expertise you need to bring an out-of-the-box BDR solution to your customers quickly, easily and profitably – without having to hire in a raft of new resources.

And while you are thinking about partnering for BDR, it may also make sense to consider partnering for NOC services too, so reducing the existing monitoring, management and remediation burden on your technical team and allowing them to focus on the new BDR service areas moving forward.

Because if your own resources are too occupied in the 'here and now' of routine maintenance and troubleshooting to focus on your customers' BDR strategies – you could be missing valuable opportunities.

Inbay partners with many MSPs worldwide to remove this burden, enabling them to focus on delivering high-value services such as BDR and build recurring revenue.

Free 30-day trial

You can register at inbay.co.uk/free-trial for a free 30-day trial for NOC services to experience what we offer at first hand: no cost, no risk and no obligation.

To find out how Inbay helped US-based MSP Adaptive Solutions to focus on those high-value items which were previously always 'over the horizon', read the full success story at inbay.co.uk/resources/success-stories.

ABOUT INBAY

Providing exceptional service to our partners' clients is our number one priority.

Founded in 2002, Inbay has been providing specialist IT support for more than a decade. During this time we have built a reputation for helping our partners to grow their managed services business by providing the highest quality service desk, NOC and project services at a fair price.

Operating on an international basis we work with Managed Services Providers who want to extend the services they offer their clients and build recurring revenue.

For more information, please visit:


www.inbay.co.uk

Head office
London, United Kingdom
45 Broadwick Street
London W1F 9QW

Telephone +44 (0)20 3435 6435
Email business@inbay.co.uk

Sydney office
Sydney, Australia
Level 14, 309 Kent Street
Sydney NSW 2000

Telephone +61 2 9994 8013
Email business@inbay.com.au

Technical delivery centre
Colombo, Sri Lanka
Evolve Tower, 82 W. A. D.
Ramanayake Mawatha
Colombo 02

INBAY™ September 2016