MSP Barracuda
Your journey, secured.

Evolving to a Security-Centric MSP

A step by step guide to help MSPs with their security journey.

WHITE PAPER

Introduction

IT Security has long been a major problem for organisations. Initially, poorly built and configured hardware meant that effective security required rafts of extra specialised equipment, much of which failed to carry out its main purpose of providing actual security. Then, poorly written code left holes that could be easily attacked by those with malicious intent. Combining the two environments led to a 'Swiss cheese' solution: one where it was easy for the supposed security to be bypassed.

Along with this were issues around accidental security issues: users sending emails to the wrong email address; using easily guessed passwords; using access devices with poor overall security; accessing systems via unsecured connections. Even internally, disillusioned employees could easily copy and remove large amounts of data before they left the organisation to move to a competitor or to sell on the market for financial gain.

Mobility only made this worse: road warriors losing laptops that could have high levels of intellectual property stored on them; users leaving mobile phones with no access security on them in cabs, hotels, cafes and elsewhere. The explosion in access via unsecured connections, both wired (mainly in hotels) and wireless (public environments such as cafes, airports) created an environment where point security solutions were rapidly being left behind.

Cloud computing has piled on to the issues: many organisations now find themselves with an owned platform over which they have a high degree of control alongside one or more public cloud platforms where the cloud owner has the greater part of the control while the organisation struggles to apply levels of security around its own part of the stack on the cloud.

The problems around mobility and security have been exacerbated through the COVID-19 pandemic. With so many people now working remotely, IT security issues have become far more apparent for organisations as they see those who are normally deskbound working from home using PCs, laptops and tablets that are not configured to an agreed organisational specification when it comes to security. This can cause a raft of two-way problems. Once data leaves the control of the corporate network, it is easier for malicious activity to gain access to that data. It is harder for the organisation to trace that data as it moves further away from its control. On the other hand, the user is creating pathways back into the organisation's controlled environment from an uncontrolled device. Trojans, worms, viruses and other payloads can be more easily spread into the environment.

Of course, the malicious activity has not stopped. We are now a long time on from the hacker just wanting to see what they could do. State-sponsored activity, from 'simple' DDoS attacks to ransomware and intellectual property theft, through to commercial groups using phishing attacks to place payloads on people's devices are getting more and more sophisticated.

This level of complexity means that organisations have a stark choice: spend a lot of time and resource that should be focused on value-add business activities on trying to keep up with everything and fight against an ever-changing security landscape, or look to others who can afford to provide a focus on overall IT security.

The three pillars of IT security

To adequately protect an organisation's information assets, a complete and well-integrated approach is required. However, this approach can be split down into three main areas, as such:

1. **Protecting users, information, applications and devices**
   Historically, many security approaches were focused on securing devices and applications. The idea here was to try and prevent the ingress of malware via access and peripheral/edge of network devices while attempting to secure applications via strong challenge and response and multi-factor authentication (MFA). The idea was to keep bad actors out of the network while enabling good actors to work without too obstacles in their way. However, the advent of cloud and the breaking down of network edges and the monolithic application has made such an approach somewhat moot. Now, the focus is having to move to how information is directly secured as it moves along the far more amorphous processes across and beyond an organisation and providing tools that secure the user from malicious activity from wherever they are accessing the IT platform. There is also a strong need to protect users from themselves: a large proportion of security breaches come from accidental actions taken by users. Enabling a means of preventing such accidents while still ensuring that users can continue to work with few (if any) hurdles to their work is an important part of an overall security solution.

2. **Provision of secure access to public cloud platforms**
   The growth of cloud usage has led to the need for such access to be secure, yet many of these clouds are not under the control of the organisations using them. Instead, users must look for strong underlying security backed with overlaying capabilities that meet the organisation's needs. Not only is this required on the platform itself, but organisations must look at how the connection between access devices or external workflows are also secured so as to ensure that there is end-to end security in place.

3. **Continuous improvement of security capabilities**
   Security needs will continue to evolve. Bad actors are in an internecine battle with the security community and new threats are hitting organisations on a continuous basis. Organisations need to make sure that their security approaches can deal with such a dynamic environment with zero-day capabilities and continuous updates. However, regular and efficient security assessments must also be carried out to both ensure that the organisation is keeping pace with its own security posture and also to ensure that it maintains a strong and effective security capability.

These three pillars should support an integrated, consistent and effective security capability where the organisation and its stakeholders can continue to work in a transparent and efficient manner, while managing to avoid both accidental and malicious security breaches.

No organisation will find that building each of these pillars separately will present them with a solid security capability: indeed, the idea is to build these as integrated supports for the organisation's overall IT platform and its workflow processes. This requires a coherent and consistent construction of an overall security solution where each tool and system is aimed at supporting one or more of the pillars.

This paper looks at all the different areas that an organisation must consider when attempting to put in place such a security capability.

Step forward the MSP

Action points

- Today's MSPs are at a crossroads: they must now move to become more aware of how security needs to evolve to meet the needs of a modern, multi-platform organisation.
- The workplace has changed: increased decentralisation of the workforce means that unowned and uncontrolled devices will become more of the norm.
- MSPs must realise that the world has changed: Control of small parts of a platform is no longer enough.
- Security has to become something that is part of the very fabric of an MSP's services.

Why the MSP is ideally situated

It is apparent that organisations are increasingly realising that procuring, implementing and operating IT equipment is no longer a core skill (if it ever was). They are also realising that writing and maintain code is decreasing as a focus. Cloud and managed services are appearing as the way forward – and the growth in MSP usage reflects this.

An MSP can only exist if it can demonstrate a capability to provide services that are better and more cost effective than the customer could do themselves. Software as a Service (SaaS) has enabled MSPs to demonstrate much faster time to market and better capabilities of responding to market dynamics, along with levels of support and availability. **Use of an underlying cloud platform has allowed for flexibility in use of resources, enabling customers to worry less about whether they will hit resource ceilings as their workloads flex**. However, aspects of security have still been overlooked.

MSPs are becoming more embracing in their approach: the relatively 'airlocked' simple services of e.g. standalone managed email and hosted apps such as accounts and contact management have evolved into integrated offerings where workflows across the platform and to and from the customer's own environment are now common. For MSPs that are still offering stand-alone solutions, it is apparent that integration with other systems is required for the future.

Moving from such 'Generation 1' services to a more flexible and dynamic interlinked set of services and functions is now the great opportunity for the MSP. Such integration must have demonstrable security capabilities, however.

Having gained the attention of the customer, implementing IT platform and data security in an integrated and sensible manner is a way to further monetise a functional portfolio.

Action steps

MSPs must prepare for the future. Security is high in the minds of the organisations who are looking to subscribe to services. Therefore, MSPs must:

- Embed security in all functions and services.
- Ensure that security solutions work in a joined-up, cohesive manner across all services, not just their own.
- Message strongly as to how they are a security-centric provider.

The need for integrated, ubiquitous security

With organisations now employing an IT platform that consists of multiple different environments, the need for security to be ubiquitous is paramount. **Any hole in a security approach leaves a probability that a malicious actor will find it and make the most of it**. It also needs to be integrated: again, a lack of integration will leave holes that can be compromised.

As such, dedicated managed security service providers (MSPs) will have less of a part to play in selling direct to end-user customers. Such security-focused service providers will find it harder to differentiate themselves in the market – particularly if general MSPs get their act together and implement security within their own services successfully. With security less likely to be layered on to existing services, the need will be for a security-centric MSP.

This can be seen as an MSP that works on the assumption that all of its services must be inherently secure; that as the service provider, they must take responsibility for what happens to the data they are entrusted with. This may involve using MSPs as a source of security expertise and services, but how those services are integrated into the MSPs own services must be managed and maintained by the MSP itself.

Further, a security-centric MSP must also ensure that the touch points between the MSP's own services and the customer's environment are secure and that they are continuously monitored and reported on, with any security issues being flagged as rapidly as possible to the customer – along with possible remediation steps.

Through this manner, **the security-centric MSP starts to provide the end-to-end security that an organisation demands: and this can be further monetised through increasingly taking more responsibility for the data flows across the organisation's own IT platform**.

Action steps

The walled garden is not a means of providing security to a customer. Proprietary systems can be dead ends that can create costly problems for MSPs. Therefore, look for the following:

- Security systems should be built to integrate with each other by default – but avoid proprietary solutions from vendors seeking to lock you in.
- Look for security systems that use open standards, making it easier to integrate different point solutions as necessary.
- Using an MSP as a provider of security services that can be integrated successfully into an MSP's platform is a valid approach.

The problems with current approaches

Current security approaches tend to be scattergun and carried out on a basis of 'once checked, everything's OK'. A primary approach is known as the 'walled garden': here, there is a presumption that an entity needs to be validated through simple means (generally a challenge/response mechanism of username and password) after which it gets full access to the application or services beyond that.

This 'walled garden' approach fails due to that although a legitimate user can get through the perimeter and can then carry on working as necessary, the same also goes for a malicious user: assuming they can breach the perimeter defences, there is nothing to stop them once they are in the environment (see Figure 1). Further, unless suitable security is built into the application or services, either entity can access things that they shouldn't really access. Obviously, in most cases, safeguards are in place to avoid even legitimate users from accessing functions they shouldn't.

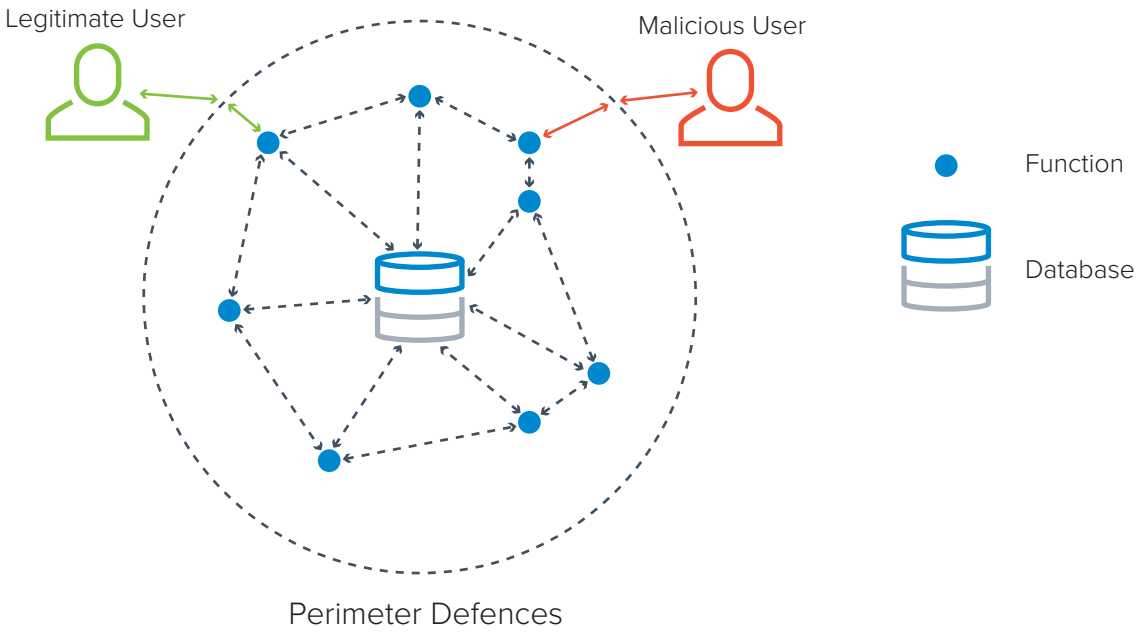

Figure 1

This gets worse when an environment consists of interrelated functions, services or apps connected via series of processes. Again, if an entity is solely secured on a simple walled garden approach, then it can move between different systems with impunity (see Figure 2).

Trying to maintain role-based security for legitimate users becomes more difficult as well: each system may have its own security mechanisms which do not match up with other system's different systems. As such, joined-up security is difficult to put in place and to manage as a meaningful overarching system.

This is not security – it is only the perception of security.

For an MSP, it becomes apparent that they must go further – a more granular and farreaching approach is necessary.

Action steps

Security needs a multi-level approach to prevent both malicious and accidental issues. MSPs must recognise that:

- Challenge and response security is not really security: once broken, any malicious intruder has full access to the environment.
- A multi-level, deeper reach approach to security is required that halts insecure activity as close to the point of activity as possible.

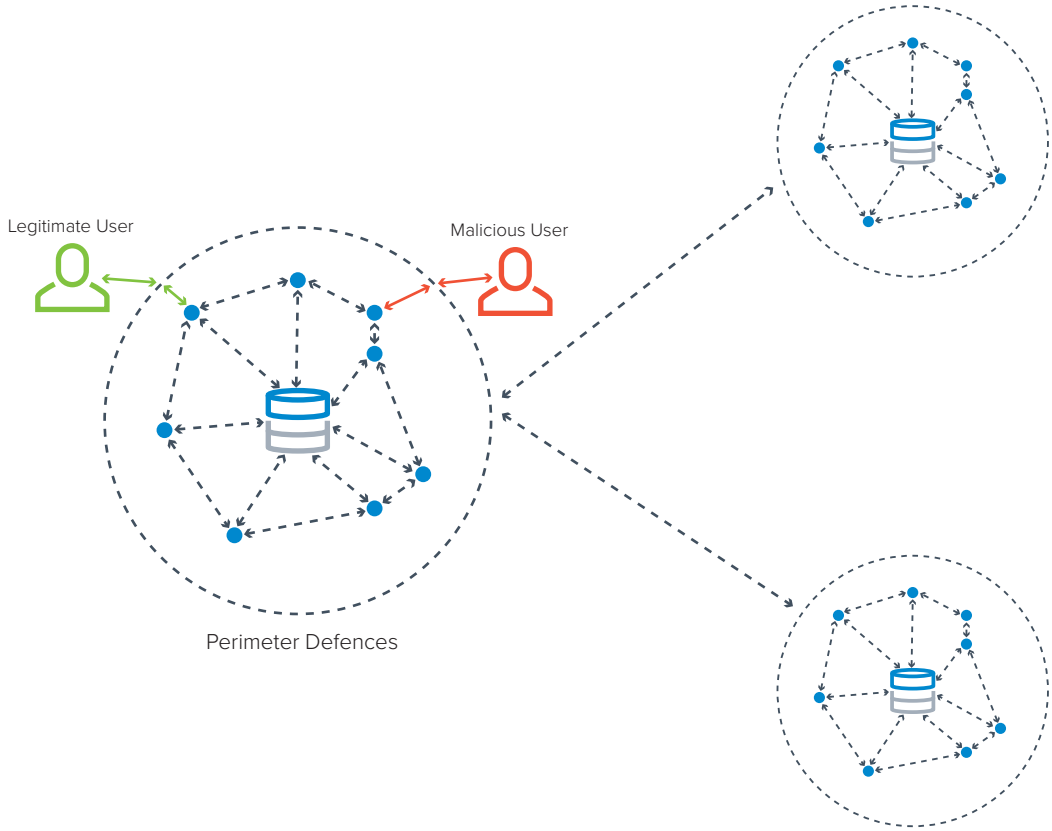

Figure 2

Securing the platform

Now, assume that the entity has to validate itself through multiple means – not just a simple challenge and response. Firstly, it has to get through some levels of access to even reach the platform itself. Edge of network intrusion detection systems can provide one level of defence here. Multifactor authentication (MFA) makes life harder for the malicious entity to get through at all.

MSPs can easily provide such MFA capabilities – although care needs to be taken in how these are provided. Phone based text messages should be avoided as they are sent in the clear. Token-based or authentication app-based systems are widely understood in the market and provide suitable levels of capability.

When the entity manages to get as far as the application, it is further challenged to validate itself – and this is then checked against a directory of users and roles that dictates what they can do within the system. Where an organisation does not have a suitable enterprise directory, an MSP can step in and become the central repository for all users, tying the customer in further to the MSP's services.

Now, it is far more likely that the malicious entity has been blocked out completely. The overall system is also far more capable of applying granular security – even legitimate users can only access parts of the functionality and data within the overall environment – driven by needs and policy, rather than hard-coded into the software (see Figure 3).

In the unlikely event that a malicious entity manages to get through both the edge of network defences and the main application perimeter defences, it will still have to pass additional verification stages as it tries to access additional services and data. Not easy.

This does require a good level of security standardisation across platforms and services. However, if MSPs provide such capabilities, then overarching systems such as single sign on (SSO) can be used to provide strong initial and ongoing token-based security across multiple platforms and services. Again, by providing such services from their own platform, MSPs start to create a very sticky environment where the customer is far more likely to stay – and take additional services.

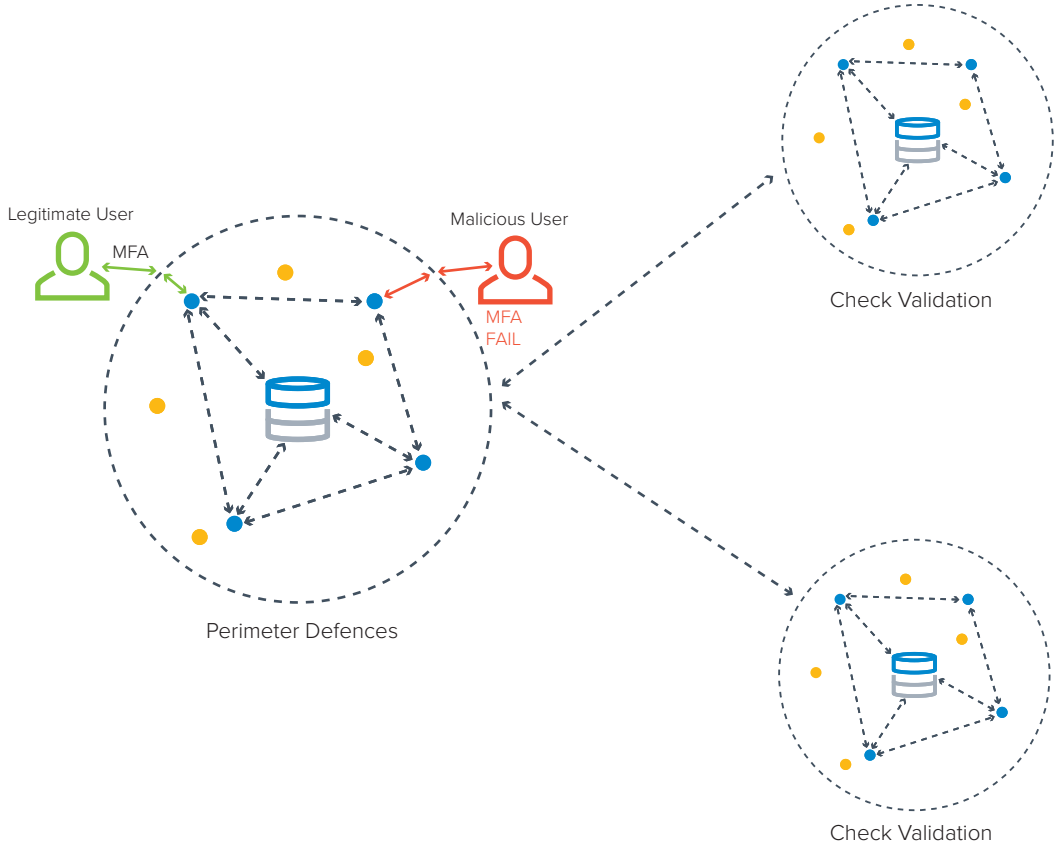

Figure 3

This becomes incredibly important when the other parts of the platform are third-party clouds. This then applies not only to how the customer accesses the primary MSP's functions, but how the primary MSP then deals with any other third-party MSP that it deals with. By ensuring that there is the capability for revalidation along the whole process flow, good levels of security can be maintained.

The processes themselves must also be secured. Some of this can be provided through regarding the process as an entity in itself. When a process requires a response from or is providing a response to a service, validation that the process is known and has characteristics that match policy (such as a known, validated user; an agreed access mechanism), then a degree of trust can be provided. However, with MSP processes often having to pass over untrusted networks, it is also important to ensure that the data within the process is secured from malicious activity.

Therefore, data tunnelling must be provided. This can be via direct encryption and/or virtual private networks. By taking data away from being 'in the clear', hijacking of the data by malicious entities becomes far harder. On top of this is the need to ensure that any data being stored at any point is secured – encryption of stored data not only at the MSP's datacentre but also at the user's premises and access devices must be provided. This then moves from the walled garden to a data-centric security approach. As data is the lifeblood of an organisation, with its intellectual property being tied up within it, this must be of a high importance.

In essence, the trick for an MSP is to provide a blended approach, ensuring that malicious activities can be blocked from accessing networks, resources and services, while also ensuring that data at move and at rest is fully protected.

Action steps

By adopting the following approach, MSPs will be better placed to provide the levels of granular security demanded by today's organisations:

- MFA provides a better level of edge security. Providing MFA capabilities should be a simple hygiene factor
- Process-based security must be the aim: becoming a process-based MSP will give the edge in the market
- Centralised enterprise directories and SSO tokens can be used to provide process transparency for users
- Contact points between different process junctions may require user revalidation
- Data at rest should be encrypted for security
- Data tunnelling via VPN or via data encryption provides security for data on the move, particularly across public networks

Maintaining information security across different organisations and roles

As well as malicious activity via external entities around security, **MSPs must also consider the areas of accidental problems and malicious activity via internal sources**. On the whole, these two areas need to be dealt with in similar ways: you don't want to put blockages in the way of individuals doing their jobs, you do want to automate data security as much as possible.

Two main areas here that help in providing a more complete security approach are with the use of data leakage prevention (DLP) and digital rights management (DRM).

DLP checks the content of data flows as they cross over significant border areas. The main way of providing DLP is through content matching – for example, any document containing a specific word or phrase can be blocked from passing across the border.

As a key area, consider emails. It is all too easy for a user to accidentally send an email to the wrong recipient. In most cases, this will not be a major problem, but when it comes to contract documents and intellectual property, it can be a major issue. DLP can be driven by policy so that emails can be checked and blocked if they do not meet corporate policy. Granularity can be added by incorporating the DLP rules with the corporate directory, for example, completely blocking certain types of information from being copied, emailed or whatever by general staff, whereas a manager may have a warning raised along the lines of "This action is against corporate guidelines. Do you still wish to continue?".

DRM adds further capabilities. Here, all information assets remain under a degree of control of the owning corporation through a requirement to check back with a central server on a regular basis. As such, even when an information asset has been moved onto another organisation's network, the receiving person can still be stopped from forwarding, printing or copying it. The information can be time limited, encrypting or deleting itself after a defined period of time.

Another aspect here is where employees who have left the organisation are concerned. Their credentials can be completely revoked and all information that they may have copied onto their own devices can be immediately encrypted or securely deleted by the original organisation. Similarly, other entities, such as complete suppliers or IoT systems can be revoked or throttled to prevent any perceived security issue from spreading into the customer's own environment.

Both DLP and DRM can be offered by MSPs as services to their customers, integrated into their information flows and edge of network systems. DLP and DRM help organisations meet the demands placed on them by shareholders, customers and legal bodies: for the MSP, such services are easily monetised if messaged correctly.

Action points

Security needs to be managed by a central system – an enterprise directory. This provides the feed for all policies and procedures around security and enables quick control of what any entity can do at any time.

- Tying into an individual's role within the organisation can provide better context to how security needs to be applied
- Enterprise directories should be a single point of reference for a person's main ID: any other roles and responsibilities must feed from this
- Preventing data leakage via DLP is a must. Such a service can be a good revenue earner for MSPs. Look for systems that work both with process flows and with email systems
- Maintaining control over information – even when no longer on a controlled network – is becoming a must have. DRM provides this and is a key value add area for MSPs

Issues with the security of third-party cloud-based service

Much of the above approach is fine when an organisation or an MSP is dealing with their own apps on their own platform. Even where a third-party cloud is being used as infrastructure or platform as a service (I/PaaS), there is a high degree of control over what security can be applied. However, once third-party services or apps are being used, then there is more of a dependence on how well the code developer has implemented their own security.

On the whole, third-party cloud platforms have demonstrated their base security credentials pretty well. However, there have been problems with the services built on these platforms. The MSP must therefore ensure that they are aware of how well the code developer and the provider manages their security. MSPs must ensure that 'real' partnerships are more than just 'tick-box' exercises. Contracts must include areas on how security is managed; how problems are resolved; how changes to systems are managed. MSPS must, as the owner of the customer, take full responsibility for whatever happens, dealing with any backend third-party issues through the agreed processes laid out in the contract.

Even where the service itself is seen as being secure, the MSP may want to take further steps in order to provide greater overall information security to their customers. A prime example here is with Microsoft 365. Although the service itself has been shown to have reasonable security, areas such as the document and email storage provided directly by Microsoft may not be sufficient to meet a customer's needs.

MSPs can offer email backups and archiving alongside management of client device ost/pst files. Backup and management of OneDrive document stores along with greater security around workflows, particularly when dealing with certain verticals may also be a requirement over and above what the Microsoft offers directly (see below). Further, O365 exchange mails can benefit from gaining domain message authentication reporting and compliance (DMARC) capabilities. Here, the details of emails are checked to ensure that they are not impersonating someone else. Now required by government departments and contractors in many countries, DMARC helps to clamp down on address spoofing (pretending the email is coming from a different person) and helps to cut down on phishing attacks and other email-borne attacks.

Action points

While the basic security of third-party services must be the responsibility of the third-party, you as the MSP must take responsibility for how issues are dealt with on behalf of the customer.

- MSPs should maintain a solid working knowledge of how third-party clouds are maintaining their security, and should report any changes to customers
- Partnerships must be deep and fully managed: contracts need to be in place to deal with how the MSP and the third-party work together and deal with issues
- The need for legal archive and data disclosure is growing. MSPs should offer archiving and search and retrieval solutions across all data and information assets
- Phishing and other email-borne malicious attacks require addressing. MSPs that add DMARC capabilities can provide distinct value-add to customers

Information security by horizontal and vertical needs

Along with organisation-specific security needs, there are also various standards around security that MSPs need to consider. At a platform level, ISO27001/2 are the most clearly defined and adopted standards around the world.

At an information level, the need for a global standard has not, as yet been met. However, there is a degree of aggregation around certain standards. The biggest one that must be adhered to by all organisations in the EU and for global organisations doing work with an organisation in the EU is the General data Protection Regulation (GDPR). The US continues to work on bringing the Californian Consumer Privacy Act (CCPA) to becoming a Federal information security standard. Many other countries and regions have also been working to put in place similar horizontal information security laws.

For those carrying out commercial transactions where financial details are involved, the laws around personally identifiable information (PII) also need to be considered. The GDPR covers PII – but not all other standards do.

However, there is also a need for organisations (and therefore MSPs) to also look to vertical-specific information security needs. For example, healthcare companies in the US must adhere to the Healthcare Insurance Portability and Accountability Act (HIPAA) when dealing with patient data – which then provides additional rules around PII. Financial services has a raft of global ISO standards, such as ISO 21188 and ISO 13491 as well as more geographically-focused ones depending on region or even country.

For an MSP looking to provide security as a core element, then the horizontal aspects of security are a must: it will be increasingly difficult to differentiate through providing such services, but the must be there just to be on a prospect's shopping list. For those MSPs who wish to focus on specific verticals, then the relevant standards for that vertical must also be included. Not only must these standards be included, but the MSP must be able to show that there is proof (via certification wherever possible) and that the certification is renewed at regular intervals to show that the MSP has maintained compliance against a changing environment.

Action points

Meeting horizontal security needs should be a given: this is unlikely to provide any market differentiation. However, vertical data security compliance can open up new market segments to an MSP.

- An MSP must be able to demonstrate adherence to horizontal data security laws. Such adherence must be demonstrably updated as necessary
- Vertical capabilities enable an MSP to pitch for specialised work: the capability to manage data according to recognised market and/or legal requirements will help close such deals

The need for security assessments

As has already been mentioned, MSPs must be able to demonstrate how their own security services have been assessed and certified. However, security does not start and stop at the MSP's perimeter. Therefore, the MSP must also assess how any third-party suppliers are managing their security as well as carrying out deep assessments of the customer in order to ensure that an end-to-end platform and information security solution is put in place.

As such, MSPs must employ the right skills to be able to go into a customer's premises and assess not only the technical aspects of the customer's platform, but also the human aspects of what is in place. Only through doing this and identifying the gaps between what is in place and best-practice security can a plan be put in place for the customer to reach that level.

This may well involve the MSP either advising on or actually provisioning new services that need placing within the on-premise environment. Although many MSPs try to avoid such on-premise work, this is the only way to ensure that full security can be put in place. However, bear in mind that such consultancy services can be highly profitable if marketed and deployed correctly.

Action points

Consultative work may not currently be a strong part of many MSPs' skills base. However, when played correctly, it can be a good margin generator. MSPs must look at how to integrate consultative services into their portfolios.

- MSPs must be able to carry out realistic security assessments of existing platforms at both the customer and supplier environments
- Employee capabilities must be built up – or partnerships formed in order to make this happen
- The MSP must be able to plug any gaps uncovered through additional hardware or software or changes to the way the customer carries out its process flows

Opportunities for MSPs

When it comes to security, there remains the need for MSPs to monetise what they offer. However, base-level security services will remain 'hygiene factor' services that only work to get you onto the shopping list in the first place. As the markets mature, even some of the more advanced security services will join this level as well. Therefore, once the basics are in place, MSPs need to focus on areas where differentiation will still be possible.

- **Customer site assessments**
  Here, the MSP will have to operate as a consultancy, applying best-practice security approaches into customers at a business and technology level.
  - Assessing the needs of the customer at an end-to-end level
  - Implementing a global individual and role directory
  - Helping to define information and overall security policies
  - Implementing suitable services and/or on-premise equipment in order to meet the overall security requirements
- **Workflow process services**
  Once information has been captured and is being processed along formal workflows, it is easier to apply security to those workflows. Therefore, full workflow services can provide good margins.
- **Additional information management services**
  Backup may not be a big earner any longer, although it is still a nice-to-have. However, proper archiving services built around backup are a must for many verticals and can be sold even into those verticals where archival is not seen as being an absolute necessity. For the vast majority of organisations, the loss of email backups and the need for legal disclosure can be very costly.
- **Information control services**
  Information is where an organisation's wealth lies. Far more than any investment in hardware or apps, intellectual property makes or breaks an organisation. As such, providing services that manage the flow of such intellectual property, such as via DLP and DRM services, can be profitable.
- **Horizontal and vertical security compliance**
  Not just as a demonstrable capability, but also as a set of consultancy services built into the site assessments mentioned above. As such, the MSP becomes a trusted partner in how the customer carries out its business – rather than just being a supplier.

Managing third-party service providers

Third-party suppliers will have their own view and capabilities around security. For an MSP looking to use a third-party service, it therefore become their responsibility to ensure that the choice of supplier is suitable for its needs. Therefore, MSPs must look for the following aspects:

- **Suitable adherence to security standards**
  The use of agreed security standards makes the integration of systems and workflows much easier. If the third-party supplier uses their own security approach, this can lead to problems down the line when anything changes.
- **Agreed approach to changes**
  As an MSP, you don't want the overall services to the customer to break down when the third-party systems change. Therefore, look for providers who are willing to work at a strategic level with you, ensuring that you have plenty of notification of changes and what they mean to you before they go live. The flip side of this is also that the MSP must be able to request changes and know exactly what is happening in the third-party – even if it is that the third-party will not be working on such a change.
- **One or more named contacts for working together**
  The lack of named contacts can lead to misunderstandings when an MSP wants to discuss certain issues. By having named contacts, along with agreed handover processes should any of these named contacts leave the company, continuity can be provided and a better working relationship created.
- **Shared data**
  In order to provide a solid end-to-end experience, it is important that all apposite data is available for analysis and action, as well as for forensic analysis should the worst happen. The MSP must ensure that sufficient access to core data is allowed in order to carry out such activities.

All the above must be included in the contract between the MSP and the third-party. Also, the contract must cover escalation processes where agreement cannot be reached on e.g. requests for changes to be made. It must also include review points and exit clauses such that the MSP (or the third-party) do not find themselves trapped in an environment that no longer works for them.

Recommendations

Security is no longer something that can simply be layered on top of existing environments. It requires a well thought through and implemented approach that covers end-to-end data and information workflows. For MSPs, this is a major opportunity – but is also a major issue. As customers continue to move to a greater usage of MSP services, the need for demonstrable security at a horizontal and vertical level will grow rapidly. As MSPs move to utilise third-party services to provide more complete services to their customers, the need to ensure that security is applied at a consistent level grows as well.

The MSP must own all issues around security. It cannot lay responsibility on to its suppliers or on to its customers. All contractual agreements must explicitly accept that security is an end-to-end issue and that any issues will be dealt with by the MSP – even if this means the MSP dealing with its suppliers behind the scenes.

Conclusions

It is a truism that security is always top of mind for customers – but that it is also bottom of pocket. For the MSP, the trick is to be able to monetise security around its services – without selling security per se. In order to do this, the services being sold need to be targeted as business services: the capability to archive and retrieve information as required; the capacity for employees to work as they want without having to understand the deep aspects of security such as encryption and accidental data leakage.

As long as the guidelines within this document are followed, MSPs should be able to provide a profitable set of services to their customers.

MSP Barracuda
Your journey, secured.