CYBER SECURITY DEMYSTIFIED

Your key cloud security questions answered

Microsoft

A QUICK GUIDE TO **THE CYBER CRIME LANDSCAPE**

*Cloud security must be considered in the context of a wider cyber security strategy. If you don't get it right, the average annualised cost of cyber crime for UK organisations is £4.1 million**

*Ponemon Institute 2015 'Cost of Cyber Crime Study'

ANATOMY OF A **CYBER BREACH**

It takes over 200 days on average to discover a cyber breach, which leaves the organisation vulnerable to repeated theft and damage during this period. The first 48 hours after discovery are critical. They demand a fast analysis of the attack, a clear assessment of the organisation's exposure and a carefully prepared communications strategy.

Not only is timing critical, but also pulling in the right business stakeholders at the right time to form an action plan

Think: How will you communicate with your staff when all your systems are down because of the breach?

1 **Planning the attack**
Cyber attackers undertake extensive research of the target organisation's technology, processes and people to identify vulnerabilities

-200 DAYS

2 **Attack begins**
Most attackers establish a 'beachhead' on the organisation's network by stealing domain administrator credentials

3 **Execution of objectives**
Having achieved broader network access, attackers can now steal information at will, or compromise key systems

4 **Attack detected!**
Most breaches aren't detected by the organisation itself, but by third parties such as banks, regulators and law enforcement agencies

0 DAYS

5 **Board informed**
The first of many board briefings and crisis meetings is held, with off-site senior executives recalled to headquarters

+1 HOUR

6 **Analysis begins**
System analysts have already begun determining the scope of the breach, particularly compromised information and damage

+2 HOURS

7 **Stakeholders informed**
First emergency communications go out internally across departments and externally to key partners, suppliers and other stakeholders

+3 HOURS

8 **Liability assessment**
As the picture becomes clearer, legal teams assess the organisation's liability and corporate responsibilities

+4 HOURS

9 **Inform authorities**
Relevant authorities such as law enforcement agencies and regulators are formally informed and kept updated on developments

+6 HOURS

10 **Full press briefing**
Preliminary press alerts are followed up by formal briefings. Senior leaders undertake media interviews

+24 HOURS

11 **Damage control**
Customer and shareholder-facing teams begin damage control, including recommendations for those affected by the breach

+25 HOURS

12 **Regular updates**
Authorities, stakeholders and media are kept informed of developments as further details of the breach and remedies become available

+48 HOURS

CYBER CRIME:
IT COULD HAPPEN TO YOU

Security professionals are no longer simply advising about countering cyber threats. New evidence indicates that most organisations will suffer a breach at some point, and damage minimisation depends on fast deployment of a robust strategy. In other words, it's no longer about whether or not you get breached, but how you respond when it happens.

LIKELIHOOD AND SERIOUSNESS

"Cyber crime is the greatest threat to every company in the world"

Ginni Rometty, Chairman, CEO and President, IBM Corp, 2015

90% of large organisations suffered a security breach in 2015

74% of small businesses were breached in the same period

HM Government 2015 Information Security Breaches Survey

"Security concerns are a primary reason for not wanting to move specific applications to the Cloud for two thirds of organisations"

Cloud Industry Forum "Cloud and the Digital Imperative" 2016

DAMAGE

"Attackers are bigger, bolder and faster"

Symantec 2015 Internet Security Threat Report

£4.1 million is the average annualised cost of cyber crime to UK organisations

70 days is the average time it takes to contain a malicious insider attack

Ponemon Institute 2015 Cost of Cyber Crime Study

4% of global turnover is the new EU fine for noncompliance with data protection regulations

METHODS

Advanced attackers:

- **Deploy legitimate software** onto compromised computers to continue their attacks without risking discovery
- **Build custom attack software** inside their victim's network
- **Use stolen email accounts** to spear-phish their next corporate victim

Symantec 2015 Internet Security Threat Report

In **60%** of cases, attackers were able to compromise an organisation in minutes

Verizon 2015 Data Breach Investigations Report

75% of large organisations suffered a staff-related breach in 2015

HM Government 2015 Information Security Breaches Survey

FUTURE OF THE PROBLEM

$150 million is the predicted average cost of a data breach in 2020

Juniper Research "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation"

82% of organisations believe their senior management place a high or very high priority on security

HM Government 2015 Information Security Breaches Survey

WHAT SHOULD YOU BE LOOKING FOR IN A **TRUSTED CLOUD PROVIDER?**

Security is an essential part of cloud services and will be the primary focus over the following pages. However, there are related areas that you should be aware of when choosing a cloud provider, namely: Privacy, Compliance and Transparency. These principles play a key role in the protection and control of your data and make up the four pillars of a truly comprehensive cloud solution. So what questions should you be asking of your provider to ensure they provide the strongest possible cloud solution?

SECURITY

A provider that's relentless about security

A cloud services provider should appreciate the wider risks to your data that security alone can't defend against. On top of the highest level of encryption and security, protecting customer content at rest and in transit, it should take a proactive approach to mitigating all forms of risk across the many different cyber threats, from malware and social engineering to state sponsored attacks and online fraud.

Ask your provider...

- How they approach and prevent wider cyber security threats like viruses, malware and the theft of information.
- Whether they are subject to independent audits and if they are prepared to share the results of these audits with their customers.

PRIVACY

A provider that knows it's your data

Your data should only be used to provide the cloud services you have purchased. Your provider should never scan your data for advertising purposes or any other reason and should ensure you control and maintain access to your data. A good provider should allow you flexibility over your operating environment, offering public cloud, hybrid and private hosted cloud options and enable you to take your data with you should you decide to leave.

Ask your provider...

- How your data will be used and whether it will be scanned for advertising purposes or any other reason.
- The level of access you will have to your data when stored in their cloud.
- If you can take your data with you if you decide to stop using their services.

COMPLIANCE

A provider that's obsessive about compliance

In order to ensure your business is as compliant as can be, you must ensure your provider not only works with regulators, but proactively engages with the leading authorities and is audited to the highest international standards by trusted third parties.

Ask your provider...

- Which authorities they work with on compliance and regulation issues.
- If they are committed to adhering to multiple recognised international standards.

For more information on Microsoft's approach to data privacy, visit this link: **https://www.microsoft.com/en-us/trustcenter/default.aspx**

TRANSPARENCY

A provider that's a leader in privacy and security

A good cloud provider should offer you complete transparency as to its actions, its commitment to compliance and its work with regulators and ensure this information is readily available to you. Protecting your data means challenging the establishment and status quo when it comes to important issues. Your chosen provider should be vocal in the industry and work with regulators and government agencies in order to meet the highest standards of data protection legislation.

Ask your provider...

- Where your data will be stored and who has access to it.
- If they are clear on how they will meet applicable data protection legislation and point you to rich resources on how they do this.
- How they would handle a third party request for access to your data.

A QUICK GUIDE TO **TODAY'S CYBER THREATS**

"Cyber threats have reached a level that no organisation can tackle on its own. It must partner with a supplier that has the expertise, commitment and extensive resources to take them on"

UNDERSTANDING **CYBER BREACHES**

The first step to improving your organisation's position is to be familiar with the possible outcomes of a cyber breach. Although they come in many forms, they generally fall into one of the following categories.

DATA EXPOSURE

Most cyber breaches involve some form of confidential data exposure, whether caused by a deliberate act or simply a handling error. Either way, an organisation's valuable information suddenly falls into the wrong hands.

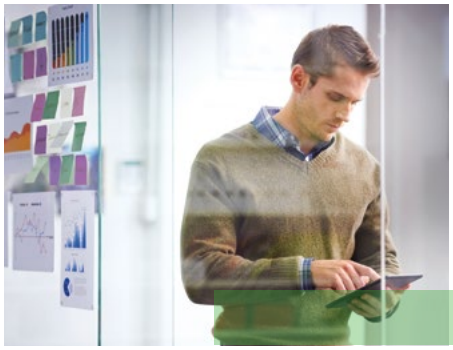
This can be information that has a value to the organisation, such as research prototypes, business strategies and proprietary processes. These are key drivers of success when privy to the organisation, but can cause great damage when exposed to competitors.

Customer data is another key target in cyber breaches, and this can put the organisation at risk of damaged public trust and extensive regulatory fines.

Deliberate data exposure has a particularly high profile at present, with cyber criminals fielding an extensive arsenal of techniques.

Traditional password cracking and exploitation of vulnerabilities are still common practice, but most cyber criminals have their sights firmly set on employees. After all, why spend hours hunting for weaknesses in a system when you can simply trick an employee into disclosing their login credentials.

Many cyber criminals now use a sophisticated mix of online, telephone and face-to-face social engineering techniques to draw information from multiple sources, which are subsequently pieced together into a bigger picture. Any confidential information can be at risk, which is why every employee has a responsibility to keep it safe.



VANDALISM

The motivations for online vandalism are no different to physical vandalism. Malicious attacks on websites, software and hardware can be for financial, ideological or simply recreational reasons.

Hacking, hijacking and viruses are key methods of causing damage, and the results are often very public and very costly to put right.

SERVICE DISRUPTION

Most breaches also have some effect on an organisation's ability to provide its products or services to customers. In this situation, businesses can suffer an immediate negative effect on income and customer confidence, while critical public service providers can find people's lives are put at risk.

The current prevalence of denial of service attacks (DoS) can be considered a form of vandalism designed to crash an organisation's online services, or flood it with so much data that customers and employees are prevented from using it. A few instances of this can be all it takes for customers to start looking at alternative service providers.

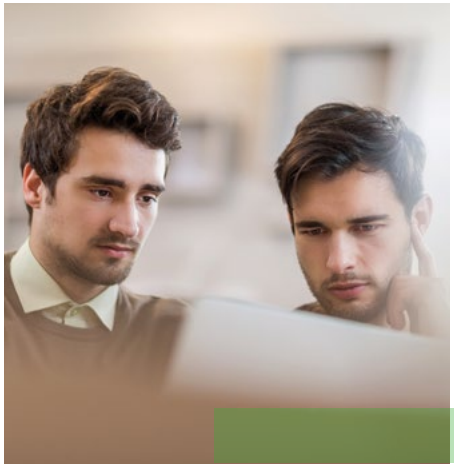
THE WHO AND WHY OF CYBER THREATS

Organisations are embracing the efficiency and cost benefits of cloud-based solutions, which is driving a huge escalation in the number of connected devices (large and small) and the complexity of networks. Less desirable is the resulting increase in risks, not simply from malicious operators searching for the weakest link, but also from inside the organisation itself. Here are some of the key external and internal threats.

External threats

INDUSTRIAL ESPIONAGE

Organisations continue to suffer direct attacks on their intellectual property, which can erode an organisation's competitive advantage. Acquiring your intellectual property could save a competitor millions in development costs, while acquiring future business plans helps them to develop effective counter-strategies to outperform you.



STATE-SPONSORED ESPIONAGE

Recent realisations about the huge scale of state-sponsored espionage are ringing alarm bells around the world. Some countries are now understood to be funding armies of hackers that target valuable intellectual property in the public and private sectors.

ORGANISED CRIME

The lone teenager pitting their wits against corporate networks may be the favoured stereotype, but most cyber crime is highly coordinated among large teams, with some groups now considered to be operating on the same scale as state-sponsored cyber armies.

ACTIVISM AND TERRORISM

Largely differentiated by ideological rather than financial motivations, cyber activism and terrorism are causing serious and highly publicised damage. Prominent multinationals make logical targets, but smaller organisations can also find themselves targeted for attack as cyber criminals hunt for the weakest link.

OPPORTUNISTS

The opportunist preys on the mistakes of organisations and individuals. Whether the motivation is financial, ideological or recreational, opportunists often look for ways to cause maximum damage and embarrassment to the victim.

MEDIA

High profile organisations often need to include media services in their list of external threats. While many operate with integrity, it's worth bearing in mind those that use more intrusive methods to deliver exclusive news and exposés to the public.

Internal threats

EMPLOYEE ERRORS

Cyber criminals specifically target employees who don't understand the threats, or even the value of the information they handle. Organisations that operate without adequate information policies or training continue to put themselves at risk. For example, only education reduces the risk of employees using weak passwords, being tricked by phishing emails, or downloading software from unknown vendors.

MALICIOUS INSIDERS

The malicious insider covers a range of scenarios from disgruntled employees to those that specifically infiltrate organisations to steal or vandalise. Naturally, appropriate background checks must be undertaken for new staff. Policies must also be in place to manage sensitive data usage, such as access being time-bound and on a need to know basis.

SUPPLY CHAIN WEAKNESSES

Cyber criminals are wise to the fact that many suppliers can't field the level of cyber resources of those they serve, which is why a growing number of high profile organisations are falling victim to targeted attacks on their supply chain. Lack of resources may mean weak cyber defences, but it can also mean a lack of adequate training that leaves bad practices unchecked, such as purchasing counterfeit software.

As a result, attitudes are stumbling a bit on devolving full responsibility, with organisations ramping up the levels of security in their supply chain.

External threats may be broader, but IBM recently found that 55% of attacks were carried out by malicious insiders or inadvertent actors

IBM 2015 Cyber Security Intelligence Index

COUNTING THE **COSTS OF A BREACH**

Cyber breaches can cause a wide range of damage, with the shape and duration of the aftermath contingent on the nature of the breach itself. Did it originate internally or externally? What information was exposed? Does it include customer or employee data? We present a flavour of the far-reaching implications as they affect individuals, the business, the UK and the world.

INDIVIDUALS

Most media coverage about cyber breaches focuses on the impacts to individuals, whether customers or employees of the organisation. There is often also a presumption of negligence on the part of the organisation before investigations have even begun.

Cyber breaches can of course cause severe damage to individuals, which is why many countries have strict data protection laws that serve to protect people from the threats caused by personal information falling into the wrong hands.

The average annualised cost of cyber crime to UK organisations is £4.1 million

Ponemon Institute 2015 Cost of Cyber Crime Study

For example, there has been a massive escalation in identity theft and fraud over recent years. Alongside financial damage, victims of identity theft can suffer spoiled credit ratings and even criminal proceedings against which their innocence must be proved.

Many breaches have also threatened direct attacks on privacy if demands are unmet, most notably Sony Entertainment, where sensitive email correspondence between senior executives was posted online.

BUSINESSES

Cyber breaches can have a severe impact on the bottom line for both the victim organisation and its supply chain. Direct costs such as system repairs and damage control can be eclipsed by indirect costs that continue to blight a brand for many years.

For example, loss of intellectual property or business strategies is perhaps the most damaging, with the worst case scenario of share value being wiped off a business as competitors bring copycat goods and services to market faster and cheaper.

As well as being damaging to individuals, the loss of personal data can be devastating for the victim organisation. Extensive regulatory fines aside, the recent Deloitte Consumer Review "Consumer Data Under Attack: The Growing Threat of Cyber Crime" revealed that 73% of respondents would reconsider using a company that didn't keep their data safe.

All of the above fuels a public relations nightmare that often demands extensive investment to restore customer and shareholder confidence.

UNITED KINGDOM

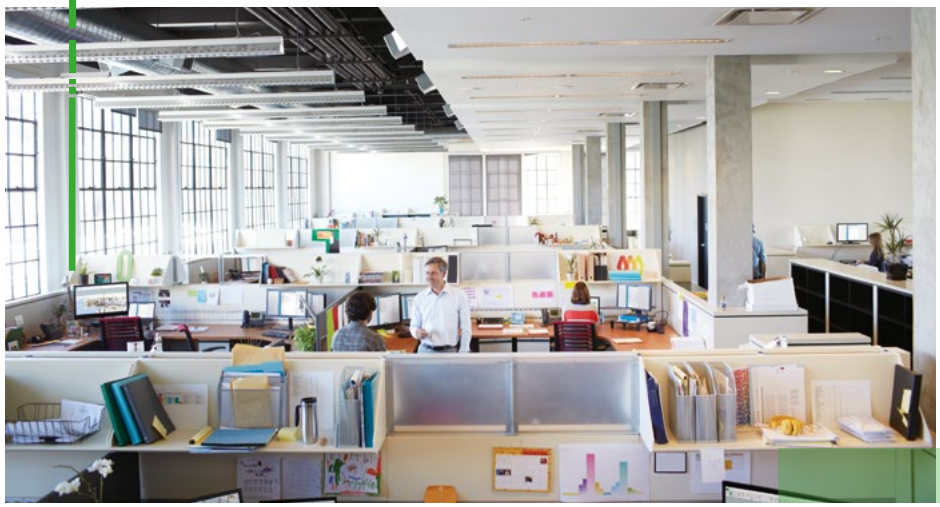
Cyber attacks now cost British businesses a total of £34 billion a year according to a joint study undertaken in 2015 by the Centre for Economics and Business Research (Cebr) and Veracode. £18 billion of that figure is attributed to lost revenue, while £16 billion relates to increased IT spend as a result of breaches. Equally worrying is that 34% of cyber crime aimed at UK organisations relates to IP theft.

The 2015 Cost of Cyber Crime Study from Ponemon Institute looks more closely at the average annualised cost of a breach to individual organisations. In 2015, this had escalated to £4.1 million, compared to £3.6 million in the previous year.

Figures like this have led the UK Government to greatly increase its cyber crime budget. However, the message remains clear that organisations must take charge of their own security, both technologically and by promoting higher levels of employee awareness.

69% of large organisations and 38% of small businesses were attacked by an unauthorised outsider in 2015

HM Government 2015 Information Security Breaches Survey



"As one of the largest cloud operators in the world, Microsoft has invested more than $15 billion in building a resilient cloud infrastructure and cloud services that deliver high availability and security while lowering overall costs."

Satya Nadella, CEO, Microsoft

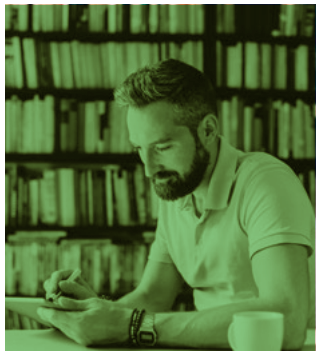
WORLD

A number of research bodies have also attempted to put a figure on the global cost of cyber crime. While this always amounts to hundreds of billions, their results are often markedly different.

The World Economic Forum highlighted the reason why definite figures are so hard to achieve, and in doing so exposed another challenge for organisations – the fact that a great deal of cyber crime goes undetected.

High profile data breaches perpetrated by highly visible groups present a clear smoking gun. In contrast, the stealthy craft of industrial espionage can be difficult to spot, and may simply manifest as a steady erosion of turnover, or be justified as an overenthusiastic target.

We'll leave you with one final figure: $2.1 trillion. According to research undertaken by market analysts Juniper Research titled "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation", the global cost of data breaches is predicted to cause this much damage by 2019.



CYBER SECURITY **IS EVERYONE'S BUSINESS**

"Championed by the board, every employee must understand the pivotal role they play in the organisation's cyber security strategy"

Microsoft

RATIONALISING **CLOUD SECURITY**

PERCEPTION VERSUS REALITY

CEOs recognise the huge transformational potential of the cloud, where enhanced efficiency at reduced costs can greatly increase the value of an organisation in the eyes of shareholders.

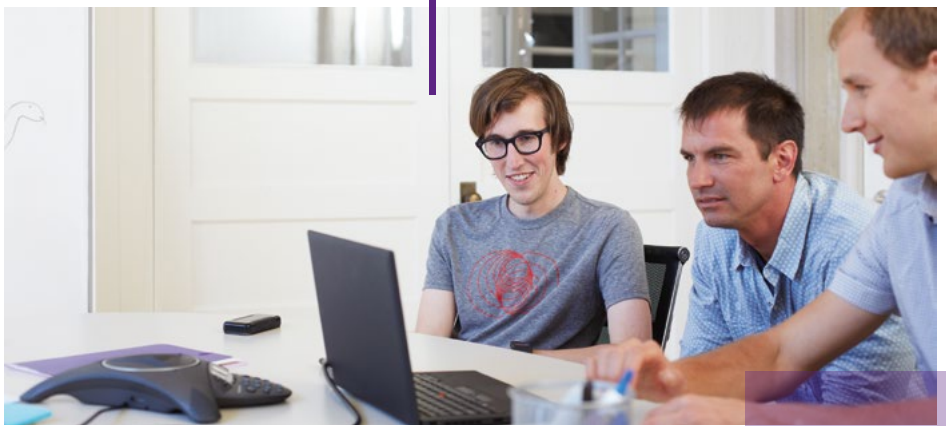
Any pause for thought is usually around the issue of cyber security, as evidenced in the Cloud Industry Forum "Cloud and the Digital Imperative" 2016 report, which found that 61% of the entire sample stated that security was a significant concern about cloud adoption, with 54% concerned about data privacy.

However, the Cloud Industry Forum also exposes a strong disconnect between perception and reality, with 98% of respondents reporting that they have never experienced a security breach when using a cloud service.

"Our research suggests that Cloud is more likely to be the solution to the security problem than the cause."

Cloud Industry Forum "Cloud and the Digital Imperative" 2016

Prompted by this and other evidence, CEOs are working with board members to rationalise fears about the cloud, not only in the context of business profitability, but also the reality of how internal and external cyber threats contribute to cyber breaches.



Microsoft

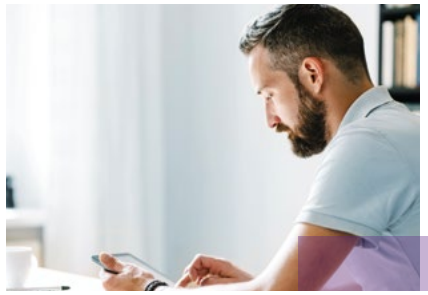
RISE OF THE CSO AND CISO

The growing interest in cyber security at board level is partly evidenced by the meteoric rise of the chief security officer and chief information security officer.

These roles have not only become pivotal over recent years, but also extremely specialised. An understanding of cyber risk and countermeasures must be balanced with strong people and communications skills to drive the employee engagement aspects. Equally essential is the ability to manage a crisis, including familiarity with public relations so they can work with marketing and sales functions to deliver effective damage control.

The importance placed on the CSO and CISO means that many no longer report exclusively through a chief technical officer. They can find themselves reporting directly to the board, and even acting as a special advisor to the CEO.

FACT
Over 80% of Fortune 500 organisations use the Microsoft Cloud



"CYBER SECURITY IS A BOARD LEVEL ISSUE THAT DEFINES AN ORGANISATION'S SUCCESS"

STUART ASTON, CHIEF SECURITY ADVISOR, MICROSOFT

An organisation's approach to cyber security will define its success in a crisis. It will define if it is going to survive, and at what cost. Naturally, this makes it a board level issue.

Minimising the damage of a cyber breach demands collaboration across the organisation. Every member of the senior leadership team must understand how their function is likely to be affected, and the role they play in designing, implementing and deploying an effective response. This must be balanced with how the organisation capitalises on the amazing business opportunities that social media and other sharing mechanisms offer.

Here, we look at the responsibilities of three key leadership roles.

CHIEF FINANCIAL OFFICER

Effects of a breach

Cyber breaches can have a devastating impact on share price, particularly if an organisation's operations are impacted or if issues of law and regulation are involved. Further financial difficulties can arise from slow manifestation of damage, which can undermine the validity of financial reports and projections for many years.

Responsibilities

CFOs must understand the value of their organisation's information. Simply put, data is an essential company asset; the value of which only continues to increase over time. Similarly, CFOs must understand exactly what would happen if that information was exposed, particularly intellectual property assets.

The CFO must support a strict approach to information classification and handling across the organisation, including driving awareness and education that ensures employees are fully aware of their information responsibilities.

Working closely with the chief security officer, CFOs must also ensure that clear mitigation and repair plans are in place should the worst occur. Specifically relating to their function, this will include measures such as timely notification of shareholders.

CHIEF MARKETING OFFICER

Effects of a breach

Marketing functions are responsible for building and maintaining brand reputation, and must be clear about the negative impact that a publically reported breach can have. Most notably, brand trust is a key purchasing point for competitors, particularly where one brand has reached parity with others. A breach could provide the negative differentiation that pushes customers towards competing brands

Responsibilities

As the communications interface of the organisation, CMOs will be responsible for managing the post-breach messages that go out to customers, shareholders and the media, including preparing board members for press interviews.

There is often little time for people to get up to speed during a breach, so the marketing function must be ready to react immediately. Deployment of the response strategy must be swift and confident, which demands advance understanding of the kinds of breaches the organisation may suffer, the security strategies in place to prevent them, and the likely outcomes that need to be addressed.

It's also worth bearing in mind that marketing functions are more likely to be involved in experimental media technologies that enable them to reach early adopters. These systems must be assessed carefully for their reliability and interoperability, with key weaknesses highlighted early on.

CHIEF SALES OFFICER

Effects of a breach

Sales forces tend to build customer trust on a one-to-one basis, which means they must understand how a breach affects individual customers. Depending on the nature of the attack, they are likely to be facing extremely concerned and even angry people. They may also be facing damaging messages from competitors that use an organisation's misfortune to their own advantage.

Responsibilities

Sales forces handle a great deal of customer information that must be protected by law. Unfortunately, the mobility of sales professionals means they are often less able to soak up the culture of cyber security that can exist among office-based staff. Awareness training is essential, particularly in key risk areas relating to device and wireless working practices. Sales staff must also know how to protect themselves from threats that working in public places brings, such as people overhearing sales conversations or seeing confidential information on their laptop screen. If this fails, sales leadership must have systems in place to limit the exposure of company information from potentially careless or negligent employees. In collaboration with the marketing function, the chief sales officer must pre-plan a clear response strategy and ensure staff members are familiar with it. Role play can be useful.

UNDERSTAND THE CYBER THREATS FACING YOU AND YOUR ORGANISATION

Although the scale and complexity of security solutions differ by sector, the impact of a breach remains very similar for all. The biggest barriers to successful cloud adoption are myths and pre-conceptions.

There is a myth that businesses in different sectors must take different actions to ensure they remain protected from cyber threats. While the type of information, processes and regulations may differ by sector, the principles of securing the business are uniform: identifying important information, protecting it appropriately, detecting threats and responding to them effectively. Likewise, implementation costs may vary between sectors, however the impact of a breach remains the same across all company types in terms of reputational and, potentially, financial damage.
The biggest challenges to adoption are myths and pre-conceptions around the cloud itself. Here we debunk a few based on a series of industry roundtables, conducted by Microsoft, across leading CIOs and CTOs.

Widespread reports of outages and breaches sap the confidence of key stakeholders, making it harder to justify the business case for cloud adoption and business transformation internally.

"We believe the cloud is more secure and understand the benefits it brings, but that is undermined by outages and breaches… it's not actually my confidence that's knocked as CIO, I just have to re-sell the solution to my board because a well-publicised outage saps their confidence."
Manufacturing Industry CIO

The perception of outages and breaches covered in the media is similar to the impact of a plane crash on the way people perceive travel safety. While horrific and widely reported, the crash doesn't change the fact that air travel is still the safest mode of transport. Despite high profile outages and breaches receiving significant press coverage, the cloud is still safer and more reliable than most on-premises environments. Cloud security should be viewed in the same way as reliability, and cloud services should be seen as a partnership between customer and service provider with both parties sharing responsibility. It is for this reason that a strong relationship and dialogue between the provider and the customer must be developed from the initial engagement, through deployment and beyond. The provider must be prescriptive regarding best practices from the outset, advising the customer of the most effective deployment in order to mitigate future issues and clarify the roles both partners will play. For example, where a customer may believe security breaches or outages are the sole fault of Microsoft, factors from the customer side, such as legacy software, human error or a lack of optimisation once the service is live, could be the cause. This is why we feel a balance of responsibility must be struck in order to create a more secure, robust and transparent solution for our customers from day one.

You and only you should be able to access your data and the data of your customers in the cloud. How would it be protected if a government came knocking?

"There are professional hackers, cyber criminals and bad people who all go after data but our customers are also concerned about Nation States and state-sponsored agencies such as the NSA and GCHQ. Is their data safe from them?"
Retail Industry CTO

Privacy and data ownership have become lightning rods in the media since Edward Snowden blew the lid on the scale of NSA and GCHQ operations. With this comes an assumption that service providers like Microsoft are complicit in handing over customer data. In Microsoft's case, this couldn't be further from the truth. We are global leaders in security, championing customer data privacy more so than any other company. If you need proof our commitment, we have sued our largest customer, the United States Government, on two occasions because we believed its request for data was invalid. Should we receive a reasonable request, we follow a specific process, working with the customer first in order to keep them informed, maintain transparency and ensure their data is protected in the right way. We are proud to put our customers' data security and privacy above everything else and are not afraid to push back and challenge the highest authorities if we feel their requests for information go against our long-standing principles. Microsoft doesn't believe technology companies should be passive on global security, which is why we are vocal on privacy issues and work with leading regulators as well as governments to help policymakers strike an appropriate balance between public safety and customer privacy. We provide complete transparency regarding our actions and will never provide any third party with unfettered access to your data. Ultimately, we start with the fundamental belief that it is your data and your data only, which means we go to great lengths to protect it.

Find out more about Microsoft's position on data privacy via the Trust Centre: https://www.microsoft.com/en-us/trustcenter/default.aspx

Without clarity around compliance and data ownership, moving to the cloud is seen as a risky move.

"We need clarity on Safe Harbour before we move to the cloud. Who can access our data? Where is our data? We need to reassure our own customers about this."
Legal Firm Partner

The announcement of the EU-US privacy shield represents a vital step in maintaining data flows and strengthening confidence in the cloud. Microsoft has not relied solely on the Safe Harbour. Since 2011, we have signed standard contractual clauses (or EU Model Clauses) with respect to our core enterprise service offerings, including Office 365. Further, we have closely adhered to the guidance of the EU Article 29 Working Party regarding implementation of the European Court of Justice decision declaring the Safe Harbour invalid as a legal mechanism for transferring personal data from the EU to the US. Our enterprise contracts incorporating the standard contractual clauses continue to provide our customers with the utmost legal certainty available for EU-US transfers. We hope that this provides you sufficient assurance that Microsoft's data processing practices align with your data protection obligations.

"Doing things in the cloud is more secure than doing [it] ourselves. It is comforting to know where your data centres are - although in government we don't always. But actually cloud providers live or die by their cloud security."

U.K. Cabinet Office Minister, Francis Maude. Cyber Security Summit 2014

At a time when doing more with less is essential, policy myths and data classification confusion are slowing cloud adoption.

"We have a real challenge moving to the cloud because some of our data is 'more OFFICIAL'."
Public Sector CTO

"Public sector data is now broken down into three categories: official, secret and top secret. As much as 87% of data is classified as official, which frees government organisations to treat it with best-practice controls used by large commercial enterprises."

Misconceptions regarding policy cause significant concerns for public sector organisations when it comes to moving to the cloud. This comes at a time when the enhanced efficiency, productivity and security the cloud provides would enable these organisations to achieve a primary goal - to do more with less.

The fact is, there are very few obstacles preventing public sector organisations from moving to the cloud now that the new government Security Classification Policy is in place. The Cabinet Office has been very clear in simplifying the process, with all OFFICIAL data now able to be stored and managed in the cloud. It is thought that up to

87% of public sector data holds the OFFICIAL classification, making cloud adoption a very real and beneficial possibility.
Some problems lie in a lack of clarity in the policy, however, producing a lack of understanding regarding data classifications. For example, OFFICIAL-SENSITIVE is often seen as data that should be dealt with differently or even as its own classification between OFFICIAL and SECRET, when in fact "sensitive" is merely a descriptor for data classified as OFFICIAL that must be treated with more care. It does not make the data unsuitable for use in the cloud.

The slow pace of policy change also causes issues for cloud adoption in the public sector, with many rules, designed before the advent of the cloud, now outmoded. For example, policy from 5-10 years ago includes rules surrounding the removal of data from the office, aimed to prevent data loss at a time when paper documents and memory sticks were prevalent. This could, of course, also apply to moving data to the cloud which, technically, means data would leave the office.

Common sense regarding outdated policy and clarity regarding data classification are essential in order for public sector organisations to make the necessary move to the cloud. The cloud itself is driving that change and it is down to providers like Microsoft to not only ensure their services are fit for purpose but to work with organisations and governments in order to make the transition as seamless as possible.

See how the government's new Security Classifications policy enables OFFICIAL data to be stored in the cloud: https://www.gov.uk/government/publications/government-security-classifications

"Public sector organisations are under increased pressure to generate cost savings, increase efficiencies and improve services, which is partly why the government has decided to embrace the potential of cloud computing."

Mark Thompson, Privacy Practice Leader, KPMG.

LEARNING FROM GOVERNMENT BEST PRACTICE WITH THE 14 CLOUD SECURITY PRINCIPLES

While designed for public sector organisations, these principles provide a solid framework for supporting cloud adoption across all industries and should be considered, alongside industry-specific requirements, as a solid framework for selecting a cloud services provider. These 14 principles also align neatly with Microsoft's 4 long-established themes for cloud services: security, privacy, compliance and transparency.

1. Data in transit protection
Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.

2. Asset protection and resilience
Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

3. Separation between consumers
Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.

4. Governance framework
The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

5. Operational security
The service provider should have processes and procedures in place to ensure the operational security of the service.

6. Personnel security
Service provider staff should be subject to personnel security screening and security education for their role.

7. Secure development
Services should be designed and developed to identify and mitigate threats to their security.

8. Supply chain security
The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

9. Secure consumer management
Consumers should be provided with the tools required to help them securely manage their service.

10. Identity and authentication
Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.

11. External interface protection
All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.

12. Secure service administration
The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

13. Audit information provision to consumers
Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.

14. Secure use of the service by the consumer
Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

DEFENDING YOUR BUSINESS FROM THE THREAT OF CYBER CRIME: **PROTECT – DETECT – RESPOND**

"Develop a comprehensive security solution and action plan to put your business in the best position to reduce risk and respond to breaches"

YOUR SECURITY IS ONLY AS **STRONG AS ITS WEAKEST LINK**

"50% of the worst breaches in 2015 were caused by inadvertent human error. Don't let your employees become your organisation's Achilles' heel".

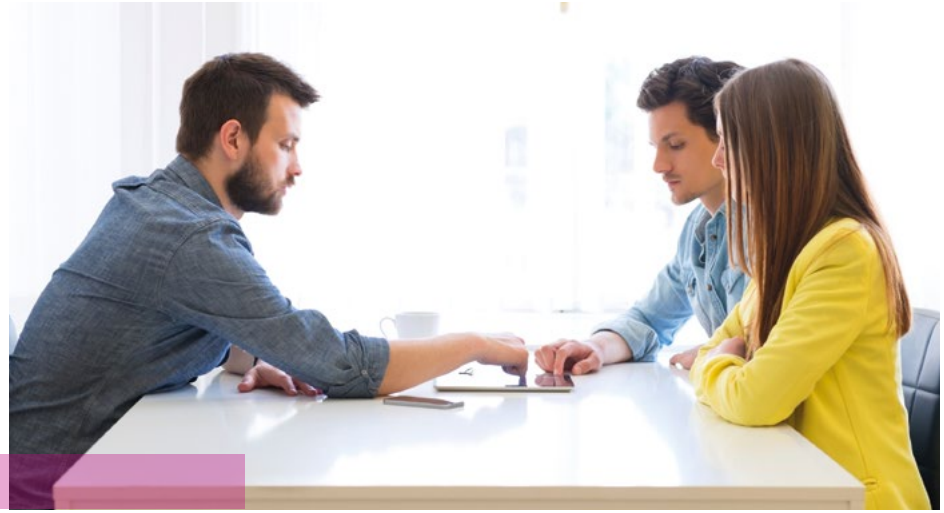
Cyber criminals are always looking for the easiest point of entry into your network. By providing fewer weak spots you will be able to make the most of the security systems you have in place.

When running your own on-premises network, the onus is on you to ensure it is protected, capable of meeting your operational needs and, in the case of customer and business information, compliant to the correct standards. With a cloud solution in place, delivered by the right provider, many of these security concerns can be more effectively monitored and managed, and the risks reduced.

75% of individuals use only three or four passwords across all of their accounts.

Source: http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email

However, high levels of security can only do so much. If you don't make use of biometric or two-factor authentication, instead



"Typically, bad people aim for the weakest point, which is the end point - old computers, mobile devices, software not updated - the weakest link is almost always the people."

Stuart Aston, Chief Security Advisor, Microsoft

choosing "ABC123" as a password which you also write down and share with others, your data won't be secure. If you run your business through cloud services but provide blanket access and control to all employees, partners and contractors, your information is still at risk. Cyber criminals use a range of techniques to access networks, from guessing or hacking weak passwords to social engineering and phishing where they use deception to elicit passwords from unsuspecting users.

5 TOP TIPS TO HELP MITIGATE THE INSIDER THREAT

- Create long, strong passwords, change them regularly and never write them down
- Use advanced authentication such as biometrics when available
- Be wary of emails and calls from seemingly legitimate entities that ask for login details and other sensitive information
- Ensure your software is updated regularly with the latest security patches installed
- Protect mobile devices with a pin, password or biometric authentication and keep them on your person

Cyber crime can take many forms. Sophisticated or opportunistic attacks are common, including infected USB sticks connected to networked devices, social engineering in the form of bogus tech support calls and even direct access to systems via stolen devices or access to computers on site.

With a greater awareness of the risks throughout your organisation, a previously weak point in your security can be strengthened.

There is a part for you and your employees to play in security, but you can be confident that Microsoft will do everything possible to play its part and beyond. The processes, training and internal policies you adopt will determine your level of protection, from employee awareness of social engineering and other potential risks, to specific guidelines implemented to ensure best practice throughout your business.

Over the following pages we will explore how Microsoft cloud solutions work alongside these best practices to enable you to better detect, protect and respond to threats.

In 2015, three-quarters of large organisations suffered a staff-related breach and nearly one-third of small organisations had a similar occurrence.

Source: PWC Information Security Breaches Survey 2015

KEEP YOUR USERS, DEVICES AND DATA SAFE WITH TOOLS **YOU USE EVERY DAY**

You can find security solutions that mitigate threats to your data and devices at the heart of Microsoft's products, starting with those we all take for granted – the tools we use every day.

WINDOWS 10

From removing the risk of hacked passwords to ensuring data stored on devices remains secure and available only to those authorised to see it, Windows 10's built in security features mitigate a wide range of security threats.

Users

With biometrics from Windows Hello and multi-factor authentication from Microsoft Passport, Windows 10 can make passwords, traditionally one of the easiest access points for hackers, a thing of the past. Additionally, SmartScreen Filter helps users make informed decisions regarding malicious websites and downloads.

Devices and apps

A range of tools within Windows 10 help to protect devices and the data stored on them, with Credential Guard keeping devices secure from unauthorised access and Device Guard and Windows Defender detecting malware and protecting devices from it with the world's largest anti-malware, anti-virus service. Windows Update for Business also ensure that the latest security software is always installed.

Data

Windows 10 includes Enterprise Data Protection, which enables automatic encryption and persistent protection for sensitive information, preventing it from being shared to and accessed by unauthorised parties.

The majority of Windows 10 and Office 365 users only take advantage of one or two of the security features available to them. Learn how you can activate the full security arsenal within your chosen products and help protect your business. Visit http://aka.ms/entst and http://aka.ms/entwfb

OFFICE 365

Designed to protect organisations from spam, viruses, malware and specific advanced threats as well as data leakage and accidental loss, Office 365 offers a robust set of security features right out of the box.

Users

Customer LockBox prevents anyone, even Microsoft employees, from accessing your data without explicit permission, while Microsoft Exchange Online Protection restricts spam emails or those carrying malware from making it inside your organisation.

Devices and apps

As malware and phishing attacks adapt and develop in order to take advantage of security software that doesn't respond to the real time threat landscape, Advanced Threat Protection (ATP) provides your organisation with unprecedented zero day protection in real time.

Data

If employees aren't up to speed with data handling policy, accidental data loss and leakage is likely. While compliance can be hard to implement at speed, Data Loss Prevention in Office 365 can automatically intervene when sensitive data is at risk, helping to keep information safe and educate users on policy. On top of this, Azure Rights Management helps to control and protect important information by enabling you to apply your own policy restrictions.

ENTERPRISE MOBILITY SUITE (EMS)

Ensuring control and security of sensitive data is essential as more employees use multiple devices and applications. Enterprise mobility tools help to secure access across devices and applications, protect the data within them and quickly identify network threats. Microsoft processes 300 billion authentications a month in its networks.

Users

With Microsoft Azure Active Directory, identities can be managed both on premise and in the cloud, enabling employees to use secure single sign-on and app self service across devices.

Devices

With so many applications and devices available to employees, the risk of exploitation also increases. Microsoft Intune provides mobile app and device management to protect corporate applications on almost any device.

Data

If your business is using legacy systems to handle sensitive corporate data, the chances are anyone can access and share it. Microsoft Azure Rights Management provides encryption, identity and authorisation to keep sensitive information safe across all devices, while Advanced Threat Analytics spots suspicious activity on your network using behaviour based analytics.

PROTECT YOUR DATA, CONTROL ACCESS AND KEEP **A VIGILANT EYE ON CLOUD NETWORK THREATS**

With Microsoft Azure, you can take advantage of the cloud more quickly while reducing security and compliance costs and minimising risk to your organisation.

Identity and access

Azure offers enterprise-level cloud identity governance, enabling complete user access control.

- Monitor access patterns to identify and mitigate potential threats
- Help prevent unauthorised access with Azure Multi-Factor Authentication

Network security

Azure virtual machines and data are isolated from undesirable traffic and users but can be accessed through encrypted or private connections.

- Benefit from firewalled and partitioned networks to help protect against unwanted traffic from the Internet
- Securely connect to your on-premises data centre or a single computer using Azure Virtual Network

Data protection

Microsoft makes data protection a priority. Technology safeguards, such as encryption, and operational processes about data destruction keep your data yours only.

- Data is encrypted when in transit and when at rest and users can choose additional encryption
- Deleted and redundant data is governed by strict industry standards that call for storage to be overwritten before reuse, while decommissioned hardware is physically disposed of

Data privacy

Microsoft is committed to safeguarding the privacy of your data. With Azure, you control where your data resides and who can access it while achieving assurance that your organisation meets its regulatory requirements.

THREAT DEFENSE

Protection from known and emerging threats requires constant vigilance, and an array of defences.

- Integrated deployment systems manage security updates for Microsoft software, and you can apply update management processes to your virtual machines
- Continuous monitoring and analysis of traffic reveal anomalies and threats—forensic tools dissect attacks, and you can implement logging to aid analysis
- You can conduct penetration testing of applications you run in Azure—Microsoft takes care of penetration testing for Azure services
- Azure Security Centre provides increased visibility and control over the security of your deployments across Azure. By tapping into the intelligent security graph comprised of billions of signals from end points, cloud applications and partners' services – it offers advanced, analytics-driven, threat detection that helps you prevent, detect and respond to security threats in real time.

Compliance programmes and certifications

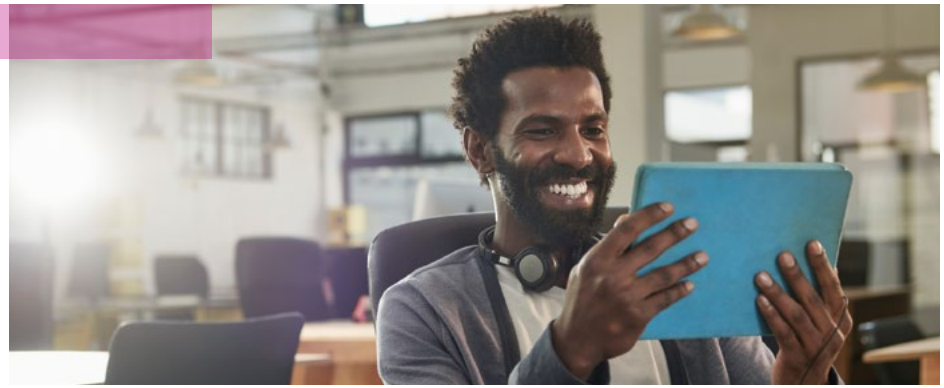
Cloud compliance is easier with Azure. By providing compliant, independently verified services, we help you streamline compliance for the infrastructure and applications you run in Azure. We also share detailed information, including audit reports and compliance packages, to provide insight into how specific regulatory standards are met.

USE ENTERPRISE GRADE SECURITY TO PREVENT UNAUTHORISED **ACCESS TO YOUR DATA**

Microsoft Dynamics ERP and CRM Online feature built-in capabilities for industry leading security, privacy and compliance, providing access only to those authorised and ensuring your data remains under your control.

The ability to view a complete picture of your business and supply chain is a game changer, but the volume of information and detailed analysis provided across Microsoft Dynamics CRM Online and ERP must also be handled securely in order to safeguard the very thing they help you to grow – your business and its data.

This is why, with Dynamics, you'll find a security model that protects data integrity and privacy while also supporting efficient data access and collaboration. This is handled by providing a convenient way to categorise users based on their job role and restrict their access to only the information appropriate to their position. However, should there be a special need, such as a group project that includes a mixture of access levels, users can be granted access to records that they don't own for a specific period. Additionally, you continue to benefit from Microsoft's key cloud security features when using Dynamics for your business, including encrypted data at rest and in transit, complete control of your data, transparent operations regarding your data and continuous compliance.



DYNAMICS CRM ONLINE SECURITY FEATURES INCLUDE:

- Field level security for sensitive data
- Support for authentication protocols: WS , SAML, Oauth
- Support for 2-Factor Authentication in Online
- Hybrid Authentication for On-Premises and Online
- Deep integration with existing Microsoft assets

Plus:

Azure ExpressRoute

Achieve increased control, predictable performance and security over your network connections with Azure ExpressRoute for Dynamics CRM. Establish a private, managed connection to CRM Online and enjoy network performance as predictable as your own on-premises environments, with most network traffic avoiding the public Internet, providing additional data privacy.

Bring your own encryption

In addition to encryption at rest, a common ask from customers is the ability to have control over the encryption keys that are used for encrypting the database. This provides great control to the customer as it enables them to change keys or revoke access on demand in a completely self-service manner. In this model, customers generate a key for encryption and upload it to a vault that they control. The CRM service then uses this key to encrypt the data for that specific customer.

Transparent Data Encryption (TDE)

Transparent Data Encryption is a great way to secure Microsoft Dynamics CRM systems, especially the sensitive information. TDE essentially protects your "data at rest", ensuring it cannot be restored on another system without a key.

PROTECT – DETECT – RESPOND

Today's cloud-first, mobile-first world demands the highest level of identity and data security in order to keep your business protected.

As has been mentioned previously, your organisation's security is only as strong as its weakest link. This protection starts with individual users who, if compromised, could reveal their identity and provide a route in to your business. With a holistic approach to security and security best practice, from the board level down to the most junior employee, you put your organisation in the strongest position to combat any threat, and there is a wealth of Microsoft solutions and services to further protect your business.

UNDERSTAND THE TOOLS AT YOUR DISPOSAL TO PROVIDE PROTECTION FOR YOUR BUSINESS:

Users

Secure your identity and access management. Understand which users should be able to access specific data and provide the correct level of access.

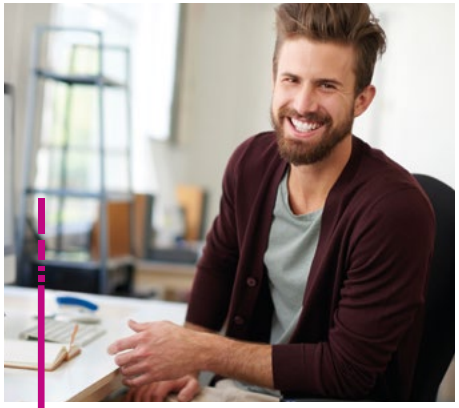
Devices

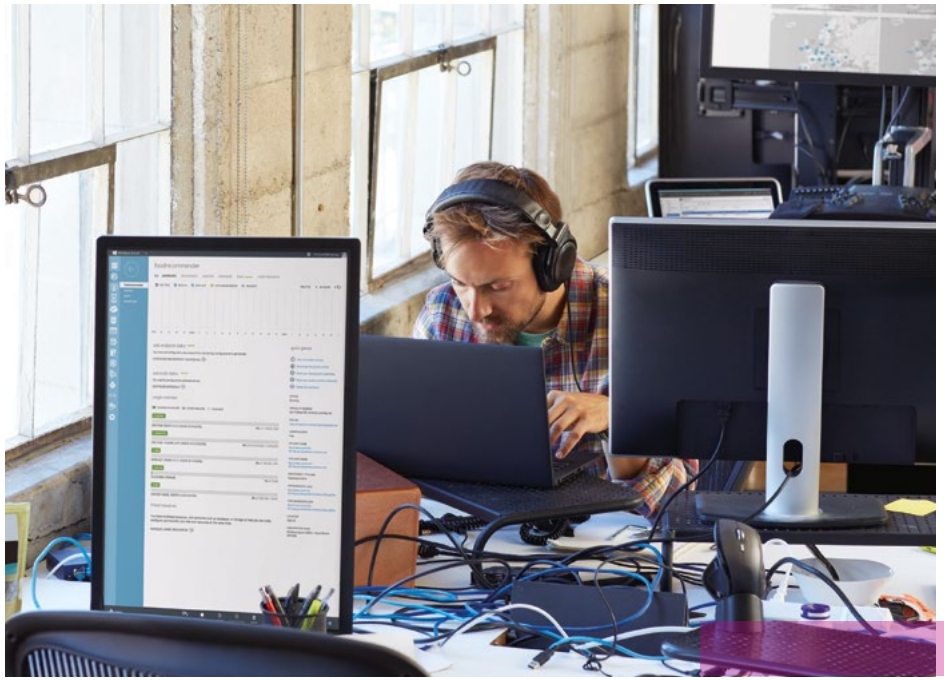
Secure your hardware, operating system and applications. Know how many devices are in use throughout your business, who uses them and for what use in order to determine access levels.

Data

Secure your data anywhere and at any time. Take control of the data across your network and on remote devices.

A holistic approach to security requires the tools to prevent unauthorised access to data, whether it's malicious or accidental, and the ability to fully manage devices and applications. It should utilise features that help to prevent common cyber attack methods, such as compromising the credentials of an individual, with advanced security features like next generation credentials, biometrics and multi-factor authentication to reduce or even eliminate this threat.





PROTECTION IN THE MICROSOFT CLOUD

Dedicated Security Tools

- Azure Rights Management
- Windows System Centre
- Windows Device Guard in Windows 10
- Windows SmartScreen

Security Development Lifecycle Services (SDL)

A free assessment of your software assurance program, delivering a roadmap to strengthen and mature your software development practices, helping you to avoid bugs and other concerns in future applications.

Microsoft Security Risk Assessment (MSRA)

Helping organisations understand their risk of exposure in critical applications and measure security controls and processes against industry practices.

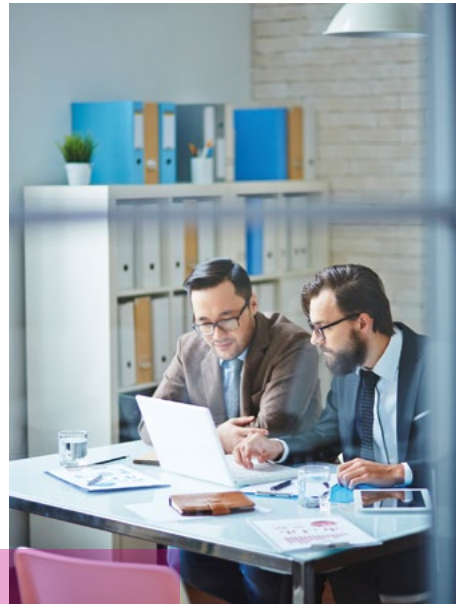
Enhanced Security Administration Environment (ESAE)

Security technologies and recommended practices to provide enhanced security protection.

Privileged Administrator Workstation (PAW) Protecting administrator credentials by adding layer of protection to administrative workstations.

PROTECT – **DETECT** – RESPOND

Don't wait 200 days to discover you've been breached. Invest in the tools and services that enable you to detect attacks faster.



In a world where cyber attacks are, on average, detected around 243 days after the initial breach took place, vigilance throughout the organisation is essential. Many detection tools aren't fit for purpose and don't catch attacks until it's too late, if at all. And even if an attack from the outside is detected, what work is being done inside network to monitor activity of those who already have access? Continuous monitoring of your network for attacks, vulnerabilities and persistent threats is required.

PROTECT, MANAGE AND MONITOR YOUR ORGANISATION'S MOST CRITICAL INFORMATION:

User

Protect users from cyber threats by providing a safe working environment complete with the latest security tools

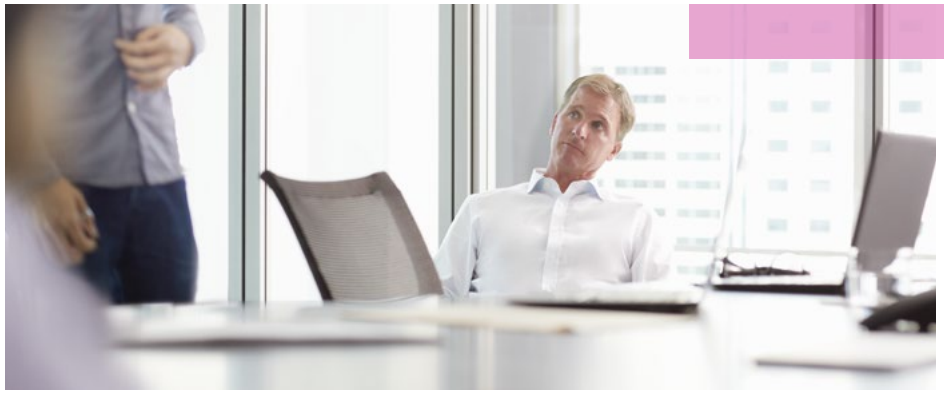
Device

Detect any deviations from baseline, policies or behaviour

Data

Detect any unauthorised data access attempts

A modern security solution should be firmly grounded in detection in order to swiftly spot and respond to cyber attacks. When a user is logged in, there should still be methods in place to determine whether their behaviour is appropriate.



DETECTION IN THE MICROSOFT CLOUD

Windows System Centre

Use Event Log to track security-related events across your network.

Microsoft Threat Detection Service (MTDS)

Detect errors and check for malicious activity while deriving intelligence to regulate and manage errors efficiently.

Persistent Adversary Detection Service (PADS)

A service that examines high value assets or a sample of systems to proactively determine whether a system is under threat.

Microsoft Advanced Threat Analytics (MATA)

Behavioural analytics and detection for known attacks and issues to help identify attacks before they cause damage.

The Microsoft Digital Crimes Unit (DCU)

Every organisation has the right to expect the technology they use to be secure and delivered by a company they can trust. The Microsoft Digital Crimes Unit (DCU) helps meet this promise by fighting global malware, reducing digital risk and protecting vulnerable populations, with an international team of lawyers, investigators, data scientists, engineers, analysts and business professionals across 30 countries. Microsoft works with law enforcement and industry, leveraging novel legal strategies to disrupt cyber criminals and, since 2010, has rescued tens of millions of infected devices connecting to more than 50 million Internet protocol addresses. This intelligence is shared with law enforcement and those responsible for critical infrastructure in a country.

Find out more at: http://news.microsoft.com/presskits/dcu/

PROTECT – DETECT – **RESPOND**

Investigate and disrupt suspicious events to provide a diagnosis and potential mitigations.

When the worst happens, or you suspect that it has, how your organisation responds and how quickly it does is essential to limit potential damage. Key questions should be answered before a breach ever occurs so that a seamless response can be put into action and a swift resolution brought about. Developing a plan and an owner to keep that plan up-to-date is an important step, as well as knowing who the key contacts are in every department. In a breach situation you don't want to be wasting time pulling together names and phone numbers in engineering or PR. You should also spend time thinking about what your approach to a breach will be; will you just pull the plug immediately or will you run a limited email service? How will you find out where the bad guys are in your system and what will you do with them once you have that information? Will you shut them out immediately and report them to the authorities or do you monitor their actions, learn from their behaviours and figure out where and how they got in? By thinking about potential ways of dealing with a breach, you'll see that simply shutting up shop and locking out intruders might not always be the best approach. Even with the best cloud security in place, you must always assume breach and be prepared to react quickly using the information and services it provides.

ESTABLISH A HOLISTIC, MULTI-DIMENSIONAL APPROACH TO RESPONSE:

User

Respond by elevating access requirements based on risk. All users should start with the minimum requirements that they need to perform their job effectively. However, if they need special rights in specific circumstances, these should only be granted for a limited time via Azure Privileged Identity Management.

Device

Respond dynamically to any suspicious device or application.

Data

Assess the impact of any illegitimate access to data, then respond to the data leak by either monitoring or removing access.

RESPONSE IN THE MICROSOFT CLOUD

Incident Response

Microsoft offers the Incident Response and Recovery service to determine whether a system is under targeted exploitation via a discreet incident response engagement. It examines high value assets or exploited systems for signs of advanced implants not typically found by commodity anti-virus or intrusion detection system technologies.

And remember... There's no silver bullet or set of golden rules for handling every breach.

As has been suggested already, even the best cloud solution can't always prevent a breach from occurring. Similarly, there's no checklist for handling a breach in general.

The nature of the breach will always determine your response, and the solutions you have put in place will simply enable you to make better decisions regarding it. That said, there are still a number of steps you can take to further prepare yourself for a breach situation, even without knowing the nature or scale of the attack. A fire drill, if you will, to help keep all individuals informed and prepared and give your organisation the best possible chance to respond.

Key questions you should ask of both your cloud services and your organisation include:

What is the risk, what is the likely motivation behind it and what could the effect of the breach be?
Are you able to dynamically adjust access based on the risk?
Does each member of your response team know the appropriate action they should be taking?
Are you, your CIO or PR team prepared to respond to media questions relating to a breach?
Are all employees aware of the situation and understand their specific responsibilities?

SEE CLOUD SECURITY IN **ACTION AT WATCHFINDER**

Discover how Microsoft's cloud solutions empower Watchfinder to grow its business, enhance productivity and increase efficiency while ensuring the highest levels of security are maintained.

THE BUSINESS

Watchfinder & Co. is a retailer of pre-loved watches, predominantly selling through its website, but also through its five retail stores located across the UK. The company was described by the Financial Times as the "leading pre-owned e-tailer" for watches and its annual turnover is in the region of £70m per year. It has a stock of over 2,500 watches across more than 50 brands, making it the UK's largest second-hand seller and is a long-time user of Microsoft technology.

COMPANY INFORMATION

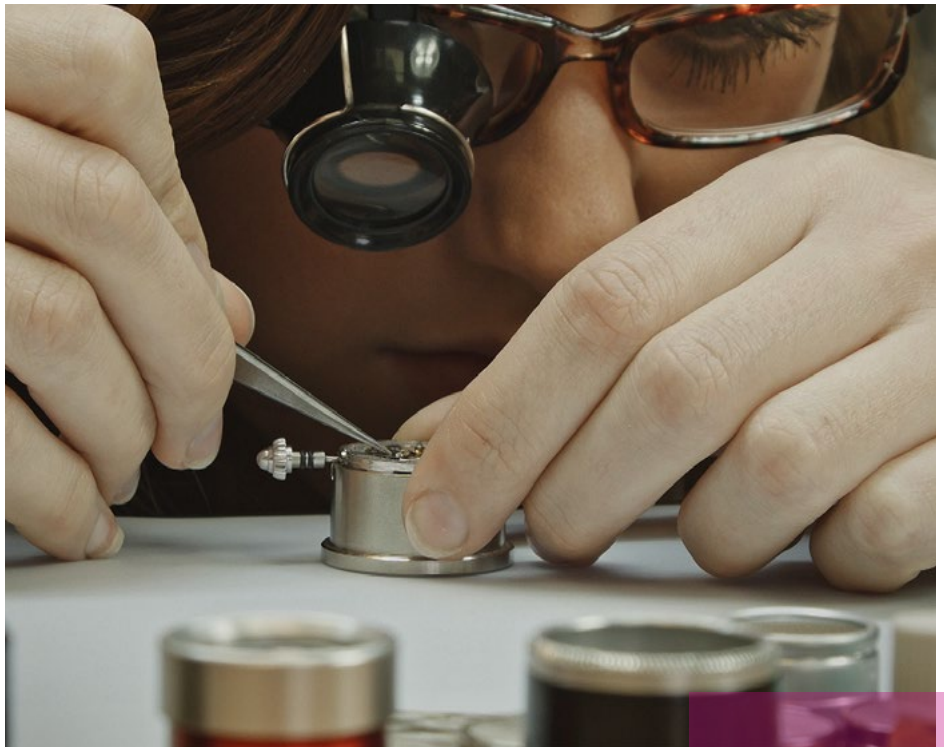
Industry: Retail/Online
Employees: 115
Location: Maidstone, UK
Retail Stores: 5 - London, Leeds, Bluewater
Online Presence: 1M Sessions Per Month

WATCHFINDER
THE PRE-OWNED WATCH SPECIALIST

MAKING THE MOVE TO THE CLOUD

Unable to find an ecommerce and sales management system to suit its unique needs as a pre-owned watch retailer, Watchfinder built its own system from scratch in 2006 and moved to the cloud as the business grew. Moving to Azure was a simple process, as IT Director, Jonathon Gill explains:

"With Azure we do things differently. You can just lift, shift and move out of your physical environment to a virtual server environment, which means the onboarding is super simple."



"We can hand over to Microsoft and their data centre management teams, who will do a far superior job than any internal team could ever do. We can leverage those skills and those resources on a pay as you go subscription model. It's perfect."

A BOOST TO THE BUSINESS

With a large amount of data generated over the life of the business, machine learning with Azure enables Watchfinder to boost its efficiency:

"We've been running for 15 years so the amount of internal data we've collected is quite vast. The power of machine learning and the Azure platform can revolutionise how the company operates. We can use this to price watches without human intervention and schedule the workflow for the service centre."

LEAVE IT TO THE EXPERTS

The move to the Microsoft clouds allays many security fears and reduces the burden of responsibility on the company's internal IT resources:

"We as a team don't have to worry about being experts in IT security, data centre physical security set up, biometrics and everything else that comes with hosting your own computers. We can hand over to Microsoft and their data centre management teams, who will do a far superior job than any internal team could ever do, so we can leverage those skills and those resources on a pay as you go subscription model. It's perfect."

SWITCHING ON ENTERPRISE GRADE SECURITY

Azure Active Directory enables Watchfinder to reduce risk with the company's internal network and passwords handled in the cloud for more secure access control:

"We use Azure Active Directory now which allows us to synchronise our internal network up to Azure which goes out to Office 365 and then we can create a single sign in environment for our staff's email. All the password management is completely out of our systems and handed over to Azure."

BETTER DETECTING THREATS

The fear of an undetected breach is reduced thanks to enhanced detection throughout the company's network:

"Advanced Threat Protection is something I'm excited about. It allows me to install agents across my internal network which use machine learning and intelligent algorithms to detect a potential breach before you do. An attack could be in your network for up to 200 days before it's discovered, ATP brings that down to hours."

PASSING ON PASSWORDS

With enhanced security delivered out of the box, Windows 10 provides the opportunity to utilise effective, modern features to do away with passwords entirely:

"I can go further now with Windows 10, Windows Hello and the biometrics that are coming through. I'm on the verge of removing passwords from the entire company. I believe passwords are one of the most unsecure ways of securing a system. By removing passwords from your staff you're removing a potential breach point."

"I'm on the verge of removing passwords from the entire company. I believe passwords are one of the most unsecure ways of securing a system."

LATEST UPDATES, FEWER HEADACHES

By moving to Office 365 the company saw immediate benefit with software kept up to date and secured from the latest threats, plus new applications and features made available as soon as they are released:

"We moved to Office 365 in 2013. I don't manage an Exchange server internally anymore which is a weight off my mind. Because it's all on subscription and we don't manage it internally, we don't need the resource to mange it, it's always up to date and we always have the latest and greatest software."

FASTER RECOVERY TIMES

Cloud storage provides peace of mind that, in the event of a hardware failure, user data is protected and can be quickly reinstated to prevent downtime:

"With OneDrive for Business we remapped documents, desktops and personal folders on their machines so if their machine breaks, we just roll another machine in, they log in, it synchronises and they're back to running how they were."

"We choose Microsoft because we trust Microsoft. They have such a support network, breadth of knowledge and range of products that you can trust them to support your business."

HOT OFF THE PRESS

Microsoft is committed to being at the forefront of security and we are excited to announce some new additions and improvements to our security suite:

CLOUD APP SECURITY – NEW LAUNCH

Microsoft Cloud App Security provides a comprehensive and proven cloud access security broker (CASB) solution which gives IT the same level of control they have with their on-premises network as their SaaS applications. Extended visibility and control allows IT to gain complete context on users, data, activities and access as well as comprehensive threat detection, prevention and data loss protection.

AZURE ACTIVE DIRECTORY IDENTITY PROTECTION – NOW AVAILABLE

Identity Protection helps customers protect their organisation from compromised accounts, identity attacks and configuration issues. The service detects suspicious activities for end user and privileged (admin) identities based on signals like brute force attacks, leaked credentials, sign ins from unfamiliar locations and infected devices, to protect against these activities in real-time. Based on these suspicious activities, a user risk severity is calculated and risk-based policies can be configured and automatically protect the identities of your organisation.

AZURE SECURITY CENTRE – NEW PARTNERS, DETECTIONS AND MORE

Azure Security Centre is adding new integrated partner solutions from Check Point, Cisco and others. Updated and expanded threat detection capabilities include the ability to detect compromised machines through crash dump analysis, as well as new network and behavioural analytics. More granular application of security policies and a new Power BI dashboard are also available.

For more information on these and all our cloud security solutions check out our Azure blog: **https://azure.microsoft.com/en-us/blog/**

WHAT CAN YOU DO TODAY TO **MAKE YOUR BUSINESS SAFER?**

Six simple but important actions you can take immediately to make your users, devices and data safer in the cloud

01	Make sure to regularly check and install the latest security updates
02	Use the most up to date versions of all software and use automatic updates where possible
03	Develop your software securely. Visit www.microsoft.com/sdl to find out more
04	Don't run software as an Administrator to mitigate risks
05	Use firewall and antivirus software to spot threats
06	Educate yourself and your staff on the latest risks, common cyber crime methods and best practice

Get your digital copy of the Cyber Security Demystified eBook at
http://aka.ms/csdebook

Microsoft