Companies are the proud owners of important, sensitive information—patented methodologies or proprietary assets that make the organization unique and valuable. These might include a confidential blueprint, a secret recipe or a trademark style.

And should those secrets be lost or compromised, it would cause great harm to the livelihood of that organization, its employees and its clients.

However, corporate espionage and other cloak-and-dagger hacker antics may not be something feared by the great majority of middle market firms as they perform routine equipment installations, provide everyday consulting services or make standardized gaskets and so on.

However, it is shortsighted to repeat this often-heard mantra: “What hacker cares about us? We have no secrets to steal. We just build widgets and what—not.”

Just because an organization isn’t the holder of a hidden treasure map, it doesn’t make the company’s data—and access to it—any less valuable to their livelihood.

What would any firm do without access to their email? Their client list? Their inventory?

What if their customer information was stolen and clients’ privacy put at risk?

Simply put, a data breach and business interruption could stymie any type of organization. Not every crook is after trade secrets. Other harmful cyberthreats such as ransomware, zero-day malware and identity theft also lurk in the shadows.

And on top of that, leaving one’s guard down can bring a world of hurt from regulatory agencies, watchdog groups or law firms that expect private information to be kept private.

That’s right, there’s the direct loss. Plus, there are fines, lawsuits and damaging public relations.

Or, if you thought the injury was bad, wait until insult is added to it.

Today, some data systems are still old school—stored and operated within legacy data servers within on-site company facilities. This is something companies may feel better about because they know their data is on-site and they can reach out and touch it.

However, much of that data lives in the cloud and more is migrating there every day—out of our physical reach. Off-site data centers house the information that keeps us competitive, viable and profitable, and many believe it is automatically backed up and protected.

But it’s not protected. Not automatically, anyway.

The cloud. And cloud security. They’re two different things, and they desperately need each other to ensure a confident state of the union regarding data protection.

PART I – TODAY’S MISCONCEPTIONS

In today’s world of IT, we must remember that the cloud and cloud security are two different things. One doesn’t automatically get paired with or guaranteed by the other.

Service and security misconceptions

There is a big misunderstanding about the differences and capabilities of software as a service, platform as a service and infrastructure as a service, and what companies are actually responsible for safeguarding in the cloud.

For example, over the past few years, many companies have moved to Microsoft Office 365 as their go-to source for email and software for business administration. So, a common misunderstanding is considering that to use a software-as-a-service offering, like Box, or some type of iCloud app, you just throw your data up there and Microsoft takes care of the rest.

First, it’s a platform where companies are just provided with a portal to host their work. Sure, they can access cloud software, yet they are the ones putting data there. Once they get it working, it’s not done. They need to configure it, secure it and monitor it correctly; this is not happening in many cases.
When there are data breaches or something goes wrong, there is no recourse if it wasn't set up correctly. There is an assumption that the cloud computing provider is taking care of everything. It is not.

Sensitive data is not just about secret formulas and corporate intelligence. It could be employee personal data stored on work devices and in the cloud. The cloud empowers end users to share files and folders with internal and external users alike.

However, what controls are in place to prevent a user from sharing an entire folder with all employee records when the goal was to just share a single file? When something happens, is the logging set up to review who did what and when? When you stand up a new Office 365 tenant, not all logging is enabled by default.

**COMING TO TERMS**

*Platform as a service (PaaS)* is development and deployment in the cloud, enabling everything from simple cloud–based apps to sophisticated, cloud–enabled enterprise apps.

*Infrastructure as a service (IaaS)* is an instant computing infrastructure, provisioned and managed over the internet.

*Software as a service (SaaS)* connects cloud–based apps over the internet. Common examples are email, calendaring and office tools.

There is an assumption that the cloud computing provider is taking care of security. It is not. Most cloud providers secure themselves, but it’s up to each client to provide their own tenant security.

Who has access to it? Is there a protected login set up or is there monitoring? One can’t just lock the door and turn off the internet at night. The data is everywhere—laptops, cellphones, iPads, etc. Likewise with a traveling businessperson who logs into a shared computer at a hotel’s business center; if that person walks away, and the account is still logged in, someone could have quick access to a large amount of sensitive data for that company.

Timeout sessions, trusted devices, protected logins—these are just a few examples of ways data should be protected but may not be.

**Data backup misconceptions**

Another misunderstanding is to assume the data is automatically backed up. As in, “Our company is in Office 365, so therefore it’s backed up.”

Just because we pay a firm to host a service doesn’t mean they’re backing up our data. They are likely replicating the data across multiple data centers to avoid any loss of data from a weather disaster in one location or a failed server, but they may not be making regular backups of the data which can be accessed if data becomes corrupted. If that data becomes corrupt, one can’t just access a different data center. The corrupt file has been replicated.

So, yes, in that scenario, there are a lot of replicated copies. All of which are bad.

Now consider this, what if it’s not your file that was corrupt? What if something went wrong with the cloud computing company providing your services?

If that provider goes down and you’re a middle market business, you may not be a priority for them. It’s simple triage—the large companies get help first.

Your data, even in the cloud, has to be backed up. It has to be backed up with a cut–off separate from a company’s network. If the network is breached, the backup is therefore separate.

Again, it must be emphasized—there is no automatic backup just because data is in the cloud. And as a result, there is no built–in recourse when a company tries to retrieve lost data that wasn’t accommodated. Check with your cloud providers for their backup policies and recovery procedures.

**Overcoming misconceptions**

There are major misconceptions about the cloud and cloud security, but these are understandable.

Not all middle market firms can justify the cost of on–staff, IT security–focused personnel or extensive IT departments.

Most of these types of companies are really all about their core business. They’re experts in their market and largely focus on what they do best, which is often not cloud security.

Therefore, they need resources that provide support for what they don’t do best. They need cybersecurity solutions for the cloud—overcoming the misconceptions that put them at risk.

**Compliant cloud–security service offerings help middle market companies focus on their core business:**

1. Cloud security helps manage data and protect it in a safe and secure manner
2. Cloud security provides remedies and recourse if situations arise
PART II – THE COMPLIANCE FACTOR

The upside is that middle market companies are getting wiser.

Cybersecurity problems, as well as solutions, are well-publicized and advertised. Some companies have gotten breached, so they’ve learned the hard way, but they’ve learned. In addition, regulatory agencies have also put the hammer down, threatening large fines if companies aren’t taking the right steps to protect themselves and others. That has gotten significant attention, too.

With that, organizations are hearing about and then asking consultants for solutions that include Microsoft security offerings. Azure Information Protection, Office 365 Data Loss Prevention and Enterprise Mobility + Security are a few of the safeguards currently available.

However, it’s not as simple as seeing an advertisement, waking up to the fact that cybersecurity is a concern and saying, “Oh, I want that.” Organizations have to ask themselves, “Does it fit our needs, does it fit our mission, does it fit our company as a whole?” Also, “Is it the right solution for us going forward?” That’s where a strategic technology consulting advisor is really going to shine—by making sure that clients get the right solution.

There is not a one-size-fits-all solution—and a big reason for that is compliance.

Consider a range of industries such as manufacturing, healthcare and banking. There are many more, but each has its own set of regulations and governing bodies.

There are intricacies that each company has with its unique form of data and data systems.

For example, some manufacturing firms work with government contracts, maybe making airplane parts for the U.S. Department of Defense. Those firms have to deal with International Traffic in Arms Regulations, or ITAR, and possibly the Export Administration Regulations, EAR. Those carry a litany of regulations and compliance standards related to cybersecurity and data risk.

In another example, health care firms are dealing with unique safeguarding and reporting requirements related to the Health Insurance Portability and Accountability Act, or HIPAA, and the Health Information Technology for Economic and Clinical Health Act, or HITECH.

Furthermore, in the financial industry, banks, credit unions, capital investment and insurance firms have to comply with reporting and risk control as outlined by the U.S. Securities and Exchange Commission or the Financial Industry Regulatory Authority, FINRA.

So, companies must manage the intricacies within their unique form of data and data systems, and then there are the reporting agencies and compliance issues they have that are unique for that business, too.

In addition, the International Organization for Standardization, or ISO, and the International Electrotechnical Commission, IEC, together outline hundreds of controls to help organizations keep information assets secure.

Also, the National Institute of Standards and Technology provides NIST 800–53—guidelines for protecting the controlled unclassified information that resides in nonfederal information systems and organizations. HIPAA is based off of NIST.

The point is, for middle market firms, it is nearly impossible to know it all. But the right cloud consultant can bring the specific knowledge for each industry.

WHERE IS YOUR DATA?

Companies may report that their data is “on the file server,” or, “it’s in Office 365.” However, it’s common to discover that it’s also in an employee’s personal iCloud account or on a recycled laptop from a previous chief financial officer.

If an employee gets that laptop and that spreadsheet showing the CFO’s bonus, it can cause great distress for an organization.

It’s critical to know where data is, and control where it can go.

The role of Microsoft Compliance Manager

To help cope with these types of compliance demands, client tenancies in Microsoft Azure or Office 365 have access to Microsoft Compliance Manager. This is an extremely helpful tool and it is displayed as a dashboard for the user.

Compliance Manager does not guarantee compliance, but using it properly can put a company in a good place to be compliant with the European Union’s General Data Protection Regulation, or GDPR. In total, the tool includes 626 controls. Forty-nine of those controls are from a physical security or architecture standpoint. In addition, the tool provides 65 controls from a virtual standpoint.

Beyond GDPR, the tool also helps with NIST 800–53 and ISO 27001 guidelines.

The Compliance Manager dashboard guides users through the control process. They take their internal paper policies and upload them to the system. In turn, it can help tenancies comply with the rules and regulations of a cybersecurity framework. Again, it is not a “fill-it-out-and-you’re-done” function, but it’s a helpful tool that companies can use to implement compliance in the cloud.

If all the Compliance Manager policies and procedures are in place...that company may be put in safe harbor if there is a breach.

As great as this tool can be, a company may not have the IT expertise to navigate it properly. However, a qualified consultant can help to connect the dots.
Compliance is essential because it allows an organization to continue doing what it does best. If a company manufactures airplane parts and that’s their passion, they need to be compliant so they can get that big defense contract.

It’s not a guarantee, but a company that has all of its compliance obligations handled properly is in a good position. If all the Compliance Manager policies and procedures are in place and an organization can prove it’s following them, then that company may be considered in safe harbor if there is a breach.

A safe harbor scenario means a company did everything it could, but it still was breached because hackers are persistent and they’re good. So, the victimized organization may have to pay for identity theft protection for its customers going forward, for example, but the government may not levy additional fines due to the safe harbor status.

**PART III – DATA PROTECTION**

A lot of companies have lost data before, so they have learned to back it up. With legacy on-site servers, backup became a very common practice that has not necessarily been lost on the cloud.

Now a company’s focus is more about protecting data. Not from a backup standpoint, but from a classification standpoint.

So, Microsoft tenancies in Azure and Office 365 all have access to technology that provides an entire life cycle of data protection tools and methodologies. Before, to have this depth of protection, middle market companies would’ve had to spend beyond their budgets—hundreds of thousands of dollars for all of the infrastructure alone. Plus, they’d need full-blown IT teams to support it all.

Microsoft now offers Azure Information Protection, Office 365 Data Loss Prevention and Enterprise Mobility + Security bundles that include the data protection companies need. No longer just for large organizations, these are solutions middle market companies can handle at a low price point. Today, companies pay per user, and not needing every aspect for every user creates a very reasonable budget item.

To apply this protection, a firm needs to know where all of its data resides. That includes data in unsanctioned locations. This could include an employee’s personal Dropbox account, for example, where a company file may be located. Such files may be used for legitimate business purposes but in a system outside of the IT department’s knowledge and control—sometimes referred to as shadow IT.

Inventorying perimeter devices, managing firewall proxies, establishing web filters, using mobile device management software—all of this helps identify the ingress and egress of data, inventorying where it all resides.

**BUT WE JUST MAKE WIDGETS**

Hackers are just scanning the internet, looking for vulnerabilities such as a company with an outdated firewall or file server box.

They may be half a world away, and don’t care that they’re attacking a small, middle-America manufacturing plant that makes nuts and bolts.

However, a ransomware attack may get that company to pay hundreds of thousands of dollars to release its data.

That’s a lot of widgets.

Unfortunately, there is no recourse. The FBI isn’t going to help. The culprit won’t be traced nor caught. It’s cheaper to just pay the ransom.

On the other hand, it’s much cheaper to pay for cloud security.

**Once data has all been tracked, a company can implement a data protection life cycle that comprises seven key tools:**

1. Classification
2. Labeling
3. Encryption
4. Access control
5. Policy enforcement
6. Document tracking
7. Document revocation

**Classification**

Classification of data is the first step and breaks up a company’s data into subsets defined as A) personal, B) public, C) confidential and D) highly confidential.

People do personal business on the clock, such as checking a bank statement. For some employees, their company laptop may also be their personal laptop in middle market companies. It may be personal, but it is data tethered to the company.

Public data is marketing material anyone can see or access.

Confidential data are things that are secret to a company.
Highly confidential data are things that are related to human resources or financially related; for example, things that companies don't want to get out.

From personal or all the way up to highly confidential data, once classified, it's all more manageable.

A firm needs to know where all of its data resides. And that includes data in unsanctioned locations.

2. Labeling
Also, once classified, data can then be labeled within those classifications. For example, if something is labeled as highly confidential, that doesn't mean everyone with that level of access needs to see it. Someone who can see highly confidential HR information may not need to see highly confidential information about an upcoming merger.

Further controls can be applied to specific labels within a classification.

3. Encryption
Encryption helps protect devices and data. If a laptop or mobile device gets lost or stolen, for example, this step helps prevent others from accessing the data on those machines.

In today’s environment where every individual has multiple devices, and where bring-your-own-device, or BYOD, is also common, there is more opportunity for unauthorized persons to gain access and encryption is more essential than ever.

4. Access control
When items are classified and labeled, then that nomenclature system helps set up and control access to the data.

That is, creating policies that can drive who gets access to what label.

5. Policy enforcement
If a company is working on a defense department blueprint then, of course, that blueprint should not be copied onto a flash drive or transferred to the same mobile phone an employee uses with his or her family.

Policy enforcement prevents those types of things from happening. For example, if someone tries to download that blueprint to an unauthorized device, an alert will notify the proper authority within the company so the issue can be addressed and controlled.

6. Document tracking
Document tracking tells the company where documents are and where they’ve been. The same applies to the defense department blueprint—the company will want to be prove that the document has never left its secure location.

7. Document revocation
Because documents are now tracked, they can also be revoked. Every time a classified document is opened, it checks in with the data protection system. So, for example, if you are on an airplane, you may not be able to open a secure document.

If there’s a dispute of some sort with the employee, the document can be revoked at any time.

The seven tools of data protection
As we now know, all data is sensitive in one way or another. Today, with tenancies in Microsoft Azure or Office 365, these capabilities no longer require a substantial IT department, a lot of infrastructure or a big budget to protect company data.