IN THIS CHAPTER

- Taking charge of cloud security
- Building a security team
- Coming up with a risk management plan
- Taking on security responsibilities
- Letting cloud service providers handle some of the security

Chapter 1
Clouds Aren't Bulletproof

All the great innovators have been known to "have their head in the clouds." Now it's your turn. Cloud computing is one of the greatest innovations of modern computing since the Internet, but with all its many benefits come certain responsibilities. One *vital* responsibility is the management of security. You can think of clouds as Infrastructure Elsewhere, but the security of all infrastructure must be managed. In this chapter, I spell out the basics of getting to know your business so that you can best create a security plan, which is the first step toward optimal application and data security when using clouds.

REMEMBER

For the most part, whenever I mention clouds in later chapters, I'm talking about public clouds, like AWS and Google Cloud. I reserve Chapter 9 for a more detailed discussion of private and hybrid clouds.

A word to the wise: When the responsibility for cloud security falls in your lap, don't panic. You'll soon find out that, with the right plan and the right tools, the task can be easily managed. To get started, you have to get to know your business. You may *think* you know it, but in order to provide truly successful security, you have to know it *in detail,* beyond just knowing the name of the person manning the front desk.

Knowing Your Business

It's great to know exactly what your business sells, whether it's widgets or services, but when it comes to cybersecurity, you need to know your business a bit more intimately. This new insight into how your business runs not only allows you to create a rock-solid security plan but also may help you innovate by better understanding how things get done. One of the first steps is knowing what you want to protect.

Discovering the company jewels

It's time to gather your first thoughts about cloud security into an actionable strategy, by understanding which assets you're trying to protect. This becomes the most important part of your plan. Depending on the size of your company, the strategies will start to differ. If you're thinking that cloud security doesn't differ much from everyday cybersecurity, you're absolutely correct. Getting cloud security right means you have a plan for all your cyberassets — wherever they live and operate.

TIP

Create an inventory of all your assets. Later in this chapter, I offer some suggestions for creating the right team. It's best to rely on them when creating an inventory of assets rather than try to noodle it out yourself.

Initiating your plan

Small companies can start their plan in a spreadsheet. You could probably get away with using a simple yellow legal pad, but then it's not so easy to share with others, and *that* is the part of the plan that comes next. Create a spreadsheet or database if you're more comfortable with it and start to list all applications used by your company. (It's easier said than done!). Many departments use applications that are hidden from the IT department. These *siloes* are towers of applications and data that are cut off from the other parts of the company — for example, accounting applications that are in use only by Accounting or sales tracking applications used only by Sales. This single exercise can be an eye-opener. You may look at the list and think, "Who is watching all this stuff?" That's why you start here.

REMEMBER

All your applications are creating and using data. Each application on your list should also include information about the kinds of data it creates or uses.

Automating the discovery process

Larger organizations might use automated discovery applications that can help you create a basic list of applications, networks, and data. This is a particularly

important first step when migrating to the cloud. For example, Amazon Web Services (AWS, for short) has an application called the AWS Application Discovery Service. (More about that service in the next sections.)

AWS Discovery Service

The AWS Discovery Service collects and documents information about the applications in use within your company and then stores that information in an AWS Migration Hub. This vital data can then be exported into Excel or certain AWS analysis tools. This is the data that underlies your ultimate cloud security plan!


TIP

AWS also has APIs (application programming interfaces) that allow you to store performance data about each of these applications. (Save room for storing the risk level information I talk about later in this chapter.)

There are two ways to gather information using the AWS Discovery Service:

- **Agentless:** This system collects data by gathering it from your VMWare application. If you have not deployed virtual machines at this point in your migration to the cloud, this system won't be useful. If you choose AWS as your cloud service provider, you'll find that AWS and VMWare are intricately interconnected.
- **Agent-based:** Deploy this application on each of your servers, both physical and virtual. The system then collects a variety of information, including the number of applications currently running on the server, the network connections, the performance metrics, as well as a listing other processes currently running.

Google Cloud Discovery Service

This particular discovery service is built into the Google Cloud. If you've already gotten started using the Google Cloud for your applications, you can make use of instance metadata, which is great for obtaining information on elements such as an application's IP address, the machine type, and other network information.

The project metadata collected by the Google Cloud Discovery Service tracks the same kind of information but includes applications that may still be running in your (physical) data center. When you're ready to tackle collecting instance and project metadata, check out the following link to Google documentation on storing and retrieving this kind of information:

`https://cloud.google.com/compute/docs/metadata/overview`

Knowing Your SLA Agreements with Service Providers

A service *l*evel *a*greement, also known as an SLA, spells out the performance and reliability levels promised to you by your cloud service provider. Though performance isn't technically part of cloud security, it's part of the overall availability of your applications and data. Your company's IT department likely has SLA agreements in place with the departments it serves. These SLA agreements depend on the cloud service providers doing their part, and they give you an idea of what they promise. For example, you can't promise 99.99 percent uptime if the cloud service provider offers only 99.5 percent. Some SLA agreements might also include references to the security they provide.

REMEMBER

One main benefit of using the cloud is that some of the security responsibility for your applications is handled by the cloud service provider. This normally includes physical security and some, but not all, antimalware security. They may additionally offer security services for hire.

Here are links to the many SLA agreements offered by some of the top clouds. Though this list is by no means complete, it gives you an idea of what's being offered and what you might expect from the cloud service provider you select or have selected:

- **Amazon:** `https://aws.amazon.com/legal/service-level-agreements`
- **Google:** `https://cloud.google.com/terms/sla`
- **Oracle:** `www.oracle.com/cloud/sla`

These service level agreements cover issues such as guaranteed uptime, disk operation efficiency, domain name system (DNS) integrity, email delivery, and more. Most of these are guaranteed at levels approaching 100 percent. Because nothing is perfect, they usually guarantee 99.99 percent or 99.95 percent for the unforeseen failures that can and do happen, but I wouldn't lose sleep over it. Statistically, you're safe with these services.

Where is the security?

One promise that's hard to track down in a cloud service provider's SLA is one concerning security. Security isn't guaranteed — just implied. Cloud service providers protect your data and applications to the limit of their ability, including issues such as physical security and some degree of malware detection by a 24/7 network operations center.

Because security is a shared responsibility, you often find that, in discussions about their security, cloud service providers talk about how they can help you create a secure cloud experience. Many of them have tools for these tasks:

- Encrypting data
- Monitoring for malware attack
- Remediating catastrophic failure

Some of the applications that perform these tasks are third-party products and services that interoperate with the cloud service provider. You generally find the partner companies listed on the cloud service provider's website.


TIP

Explore the security and service offerings of companies that are partnering with your selected cloud service provider. These companies are usually certified and provide a seamless software experience.

Knowing your part

When it comes to cloud security, the ball is primarily in your court. It's up to you to decide whether you have the company resources needed in order to provide the necessary security services. You can also choose to contract with a third-party service provider. They generally offer security monitoring and in some cases also provide applications for identity and login management.


TIP

Consider using an artificial intelligence (AI) security framework. Chapter 7 goes into more detail about how using *a*rtificial *i*ntelligence for IT *op*eration*s* (AIOps, for short) can help you integrate your cloud security into your overall cybersecurity using big data to recognize data intrusions and speed up resolutions.

Building Your Team

One part of security planning that's often overlooked involves the important step of building a security team. The people on the team don't need to be security or cloud experts, but they need to understand the kinds of applications and data that your company is running in the cloud. Your success depends largely on putting together the right team, so this section talks about putting together that team.

Finding the right people

It's true that data security issues normally cross boundaries within a company: Different departments or groups run different applications, have different security requirements, and possibly follow some different legal data protection requirements. For cloud computing environments, this is even more true — cloud computing not only spans the various parts of your company but is also, in most cases, hosted outside of your company's data center. This increases the responsibility of managing the security of the various parts of your cloud environment.

The people you want on your team will help build your security plan and later make sure that it's implemented within their neck of the woods. Because these team members will work closely with the people using the cloud applications and associated data, it often becomes their responsibility to do the housekeeping to make sure their coworkers are following the best security practices. They don't just wander around looking for "sticky notes" with passwords stuck to monitors — they educate, they do some of the policing, and they further the objectives of the plan they help create. This strategy spreads the responsibility for cloud security throughout the entire company.

Including stakeholders

When talking about stakeholders, you might have a tendency to look around the room during a meeting to spot people you think may be interested in being responsible for cloud security. Choosing the right stakeholders is a bit of an art. Getting the right people on your team is important for maximum success. There are a number of stakeholders you might not have imagined that can be involved when using cloud services, including these:

- **Cloud service providers:** These are the companies providing the actual cloud services, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platforms as a Service (PaaS).
- **Cloud carriers:** These are the telecom companies providing access to the cloud services. They are often forgotten but are quickly remembered whenever their systems fail. Cloud service providers can promise you 99.99 percent uptime, but if the cloud carrier fails, the promise is moot.
- **Cloud brokers:** These companies provide value added services on top of cloud service providers. You can think of them as packagers. They're important because the value added services they provide can cover areas such as security and identity management applications.

- **Cloud auditors:** This one is exactly what it sounds like — third-party services that audit your systems to make sure you're complying either with items such as your SLA agreements or with regulations safeguarding your data.
- **Cloud consumers:** This one consists of you and the people in your company. You and your company's end users are an important part of developing your security plan.

TIP

Find a contact, within the organization, from each of the various cloud service providers you use and make them part of your team.

When selecting company stakeholders, you might be tempted to choose only department heads to be on your security team. In many situations, they are not the people most familiar with the applications and how they're used. For example, department heads might not know which external applications are being accessed via an API, and they may not be up to speed on the level of security involved in managing the credentials used to gain access to the API.

Find the people who are using the applications and data — the *actual* stakeholders, in other words — and put them on your team. This strategy does two things:

- It involves the people most likely to be impacted in creating and knowing the security plan. That way, it's not handed down to them in a memo that gets "filed." Instead, they have a personal stake in making the plan work.
- It lets the employees who are most familiar with the applications and data they use every day know who needs what level of access to which applications.

TIP

Hold group meetings (Zoom is just one option) and select your stakeholder team members based on their level of interest, excitement, and knowledge.

Creating a Risk Management Plan

After you've put together your team, it's time to get to work. After the obligatory icebreaker "What's your name, which department do you work in, and where's your favorite lunch restaurant?" the real work of creating a security plan starts.

You can't begin protecting something when you don't know what you're protecting and how much protection it needs. Not all applications and data are created equal. Some may require access limitations to only a few people and need special encrypted communications, whereas others may require a simple username and

password for access. Get started by creating a simple diagram, as shown in Figure 1-1, that will give you an idea of where your risks may be lurking. This section covers some of the basic strategies for creating a risk management plan.

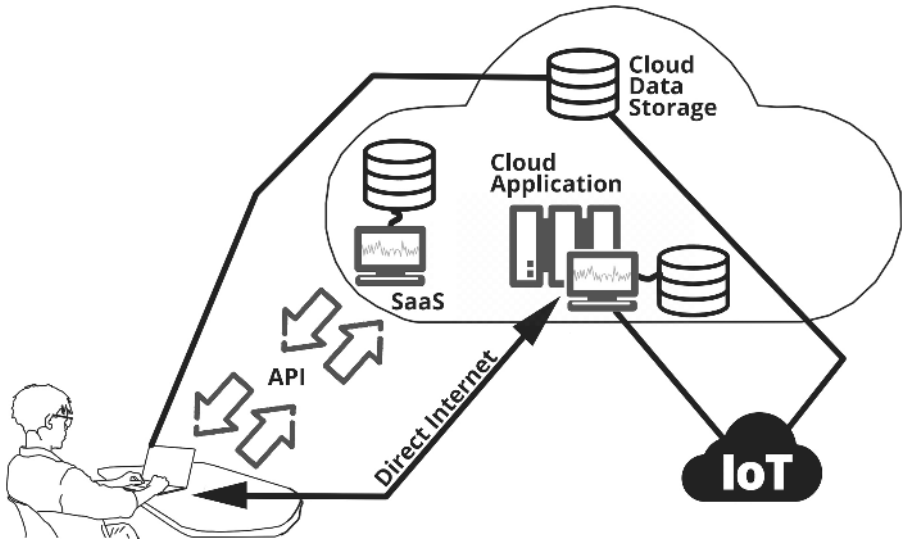

FIGURE 1-1: Map applications, APIs, data storage, and IoT devices.

Identifying the risks

If your relatively small business is looking to document the security risks you're facing, you can probably start with just a simple spreadsheet. If you have many assets, you might consider either having your developers put together a database application or use one of the commercial asset management applications.

REMEMBER

Asset management applications differ from configuration management database applications. Although they can overlap in some areas, their focus is quite different. Asset management applications deal with *assets* — anything that has value, in other words (admittedly, a fairly broad definition). A configuration management program manages *c*onfiguration *i*tems, or CIs — those items one uses to successfully complete the much narrower task of delivering an IT service. So, CIs are assets, but not all assets are CIs. An asset might be a knowledge base, but not be important enough to be managed as part of an IT service. *C*onfiguration *m*anagement *d*ata*b*ase applications (also known as CMDBs) are covered in greater detail in Chapter 7. Spoiler alert! CMDBs are cooler than asset management programs because they track how various systems interoperate with one another. When it comes to risk management, knowing how stuff works together is the key.

TIP

Most *c*onfiguration *m*anagement *s*ystems (CMSes) can generate a service map showing dependencies between systems. It's pretty cool.

For now, put together a list of the assets that are critical to your operation. You can worry later about what kind of software program manages them.

To get started, list all your assets, including these:

- Cloud data storage
- Local data storage
- Cloud applications
- Local applications
- Data repositories accessed via APIs
- Computers, mobile devices, IoT devices
- Other compute devices

TIP

When documenting your assets list, it helps to list the location where each device might be found. This includes specifying whether it's a local physical location or in the cloud. (And, if it's in the cloud, be sure to say which one.)

Assessing the consequences of disaster

No one wants to think about consequences, but in order to prepare for eventual catastrophes, you must know what potential events might occur. Carefully think about the risk involved for each asset. Ask yourself questions such as, "If this device were compromised, or destroyed by malicious hackers, what would do I stand to lose?" Put this assessed risk into a column or database field.

TIP

Assigning a numeric value to the potential risk allows you to create some useful visuals, as covered later in this chapter.

Pointing fingers at the right people

After you have an idea of the risk involved with each asset, you should assign that risk to the team member best capable of managing that risk. Spell out the roles and responsibilities involved with managing the risk.

TIP

Don't dump all the responsibilities on one person, or even on a couple of people. Spread them out so that no one gets overwhelmed, particularly if things start going wrong. You don't want one person trying to manage a potential catastrophe.

Create a role-based responsibility matrix. That term sounds like a mouthful, but it's simply a list of responsibilities, a description that lays out both what's involved in the responsibility and who's assigned to manage it. They may also have people on staff who ultimately take on the assigned tasks.

REMEMBER

Perhaps the most important step in creating the plan is to figure out how not to fail. Think of the things you need to do to prevent, to the best of your ability, bad things from happening. Perhaps this strategy involves limiting data access or ensuring that access occurs only by way of an encrypted tunnel.

Disaster planning

If all the steps you take to avoid disaster are successful, you might never need to implement contingency plans — but you should have such plans on hand anyway. What will you do if the nightmare becomes real and you're faced with a situation such as a ransomware attack, where all your data is locked up and the bad guys are asking for millions in Bitcoin? Maybe a hot backup with different security protocols running in the background that you can quickly switch to can do the trick. Maybe not. The thing is, you simply have to be creative in coming up with a solution that you know will work, given your particular circumstances.

REMEMBER

Keep in mind the old saying "No risk, no reward." Risk is something that should be managed — few things come without risk.

In your risk assessment plan, meet with the stakeholders and talk about the information you've put together so far and decide how much risk you can actually live with. The first solution you suggest — a hot backup, for example — may be too expensive or too much work to be feasible, but stakeholders need to be aware that, without it, there is higher risk. And neither is it the case that a shutdown is all you have to deal with. Customer trust can fly out the window if all their personal financial details are released to the world, or at least to the world of people trying to exploit it.

REMEMBER

Managing risk isn't a one-time endeavor. It's a challenge that you have to constantly focus on because risks change. New exploits are created. Staff turnover can create new risks if the new hires are uneducated in the security procedures you've put in place.

When Security Is Your Responsibility

When you finally have worked out the details of your cloud security plan, you still have to put that plan into action. Being responsible for cloud security is a bit like being a circus ringmaster: You're sure to have irons in many fires at a time, and a bit of juggling may be going on.


REMEMBER

Your security plan is not a dead document. It's meant to be enhanced, revised, and ignored on weekends. (Okay, maybe not the last one.) Revisit the plan often to make sure that your asset list is up to date and that you have an accurate understanding of the risk level of your various assets.

Determining which assets to protect

Earlier in this chapter, I suggested breaking out a spreadsheet and creating an application tracking your applications by entering them into the spreadsheet, but in the end it's probably more cost effective to just use an automated asset tracking tool. These tools allow you to keep your list of assets up to date daily — something you probably couldn't do manually, or at least wouldn't want to.

These are the assets you track:

- Software applications
- Computer hardware, including mobile devices
- Networks, both hardware and software based
- Internet of Things devices or other technology devices

Using an automation tool

An *IT asset management* tool (also known as an ITAM because everything IT needs its own acronym) is a software tool that allows you to track all your company's technology assets. It's a bit like the spreadsheet I describe earlier — but one on steroids.

ITAM tools track detailed information such as the purchase price, maintenance costs, repair costs, and device manufacturer. This is important information, particularly as part of a disaster recovery plan.

You have to know where everything is at any given moment. Because people are the greatest threat to security, you want to know where all those employee laptops and mobile devices are and what condition they're in. Do they have the latest security patches? Are all the licenses up to date? Are passwords being changed regularly?

Contractual information is also tracked in an ITAM tool. You can track warranty information, licenses, support agreements, and any terms and conditions for use, particularly for software assets.

Letting ITAM help you comply

Many companies must work within different security compliance regulations. For example, SOC 2 compliance can give your company an edge when working with sensitive customer information. (For more on SOC 2, see the nearby sidebar, "SOC 2 in a nutshell.")

SOC 2 IN A NUTSHELL

SOC 2, the number-2 variety of *s*ystem *o*rganizational *c*ontrol, is a best practices audit to make sure that your business-to-business (B2B) services are secure and trustworthy. Becoming SOC 2 certified lets the businesses you work with know that they can depend on you to secure their information. The trust service criteria include the ones described here:

- **Security:** Securing access to information
- **Availability:** Making sure your systems are up at least 99 percent of the time.
- **Process Integrity:** Maintaining data change authorization
- **Confidentiality:** Keeping sensitive information safe
- **Privacy:** Securing data lifecycle management

Becoming SOC 2 compliant isn't an overnight process. It can take up to a year to get your policies and procedures in place to guarantee the level of security SOC 2 requires. This is more than just a piece of paper: When you do business with a company that is SOC 2 certified, you can have a high degree of confidence that its leaders have done the hard work of making sure your data remains safe.

Applications designed to manage and protect your company's assets

Spreadsheets and databases can be great risk assessment tools for smaller business, but if you have a larger company with many assets, you may want to get started immediately using an automation tool to automatically discover your assets, and update your CMDB or asset tracking system, and then manage assets with greater visibility. You can also find applications that will assist you in discovering vulnerabilities in the overall *attack surface* — all the points an attacker might gain entry into your system — and alert you to fixes or, in the case of AI deep learning systems, will automatically repair the problem before it even rears its ugly head.

This list details a few of the major applications, to get you started:

- **Qualsys (`www.qualys.com`):** Here's a company offering a whole suite of applications for asset tracking, cloud and IT security, and regulation compliance. The (free) asset tracking app does global IT asset inventory and discovery. Its goal is to make everything visible. Qualsys also offers several applications for threat detection, a CMDB for configuration item tracking, an inventory of digital certificates, and a cloud security monitoring app, among others. The cloud security monitoring app continuously monitors cloud assets and resources for misconfigurations and nonstandard deployments.
- **Ivanti (`www.ivanti.com`):** With Ivanti's tools, you can use AI to discover problems with your cloud assets. In fact, you can automagically discover and fix problems before they even become an issue. That's the great thing about deep learning and AI; Ivanti tools comb through massive amounts of data in order to spot things that are acting out of the ordinary and then either alert you or automatically fix the problems. This is the essential use of AIOps.
- **Tanium Asset (`www.tanium.com/products/tanium-asset`):** Visibility is a vital part of managing complicated cloud environments. Automating asset discovery and being able to see your assets and how they're performing is critical to efficiency and success. The Tanium Asset application is up to the task, even feeding real-time information to your CMDB so that you have the most up to date configuration information available.
- **Tenable.io (`www.tenable.com/products/tenable-io`):** Tenable is a risk-based vulnerability management SaaS application. As such, it gives you a view of where vulnerabilities might exist and the risks they pose. After scanning your entire network, it can suggest ways for you to shore up weak points. It also integrates with a CMDB — without having to use scanners or agents. Their vulnerability assessment can provide information as short-lived resources scale up and down, something often missed during normal vulnerability scans.

» **Detectify (**`https://detectify.com`**):** This suggestion isn't an asset management application per se, but it still helps you protect one of your most important assets. One point of weakness for many companies is the website. Though this isn't the number-one asset weakness, it's likely number two — and it's public-facing. One thing you can do to test your website for vulnerabilities is to *pen*etration-*test* it (known as *pen-testing*). Many software applications out there can assist you with this process — Detectify is one of the better apps out there. It scans your public-facing websites, looking for vulnerabilities, and offers suggestions on how to overcome them.

Knowing your possible threat level

When figuring out the risk for each of your assets, set up a standardized threat-level metric that works for you. You can also use the standard shown in Table 1-1, if it's easier.

TABLE 1-1 Risk Levels

Risk Level	Asset Type
Low	Public data, such as an informational website
Low	Easily recoverable systems that contain no confidential information or critical services and are not networked to higher -risk networks
Low	Runs noncritical services
Medium	Contains confidential or internal-use-only data
Medium	Network-connected to other medium risk networks
Medium	Provides important services or information important to business operations, but not enough to stop or severely damage the business
High	Contains secret, financial, personally identifying information
High	Contains data restricted by compliance regulations, such as medical records or financial and credit card information
High	Provides business-critical services
High	Networked to other high-risk networks.

REMEMBER

It's easy to overlook systems, servers, or devices that may not contain any confidential information or critical services themselves but are networked to systems that are higher risk and contain risky information. The seemingly low-risk system may act as a gateway for unauthorized access to the higher-risk information.

TIP

Different regions of the world have varying restrictions on privacy and different compliance regulations. The European Union is a good example of an area with higher privacy regulations and "the right to be forgotten." Companies that maintain public information, like Google for instance, are required to remove private information at the request of the person to which it refers. In other words, if you don't want to appear in a search, you can have that searchable information removed, maintaining your privacy.

Van Gogh with it (paint a picture of your scenario)

A picture is worth a thousand words. Making your risk assessment simple to read and easily understood by those responsible for protecting systems is best done with a heatmap.

A *heatmap,* with colors from green to red, allows you to quickly assess the risk and dangers involved with each possible security breach or system failure. Figure 1-2 gives you an idea of the color scheme you might use in creating a heatmap. Even here with the scenarios laid out, you can see that the deep red is reserved for only the riskiest scenarios and represents a lower percentage of overall risk.

FIGURE 1-2: Color maps help visualize your risk landscape.

Giving each color a numeric value allows you to do things like sort your spreadsheet based on overall risk. You can see in Figure 1-3 that the values show the highest risk quickly and easily. Giving each risk a numeric value also allows you to export this data to other applications that will help evaluate and monitor your risk.

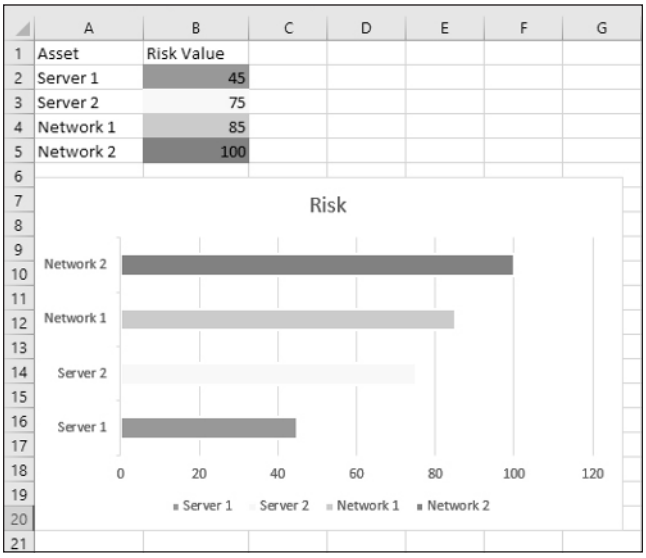

FIGURE 1-3: Simple spreadsheet heatmap shows the highest risk.

TIP

For more complicated heatmaps, you can use an off-the-shelf heatmap generation application. They come in all shapes and sizes, including ones you can integrate into a map for geopositioning. (Check out Balbix at `www.balbix.com/insights/cyber-risk-heat-map/`.)

Whatever you can do to make concepts visual makes them simpler for your team to understand. When it is possible to have your heatmap updated automatically, you'll have a resource that is useful in an ongoing way, rather than just a planning tool.

Setting up a risk assessment database

Determining what to do when things go wrong is one of the most important steps you can take to fend off a true disaster. The most important question you need an answer for is, "What happens when confidentiality is lost?" This loss might be caused by hackers, an accidental data release from a program error, or the inadvertent publishing of data to the web.

TIP

More damage is done by trying to cover up a data breach than by the breach itself. It's a difficult task to own up to this kind of security failure, but it's the right thing to do.

Confidential data loss

You should make a plan to deal with confidentiality loss, even though it may seem like trying to close the barn doors after the horses have escaped. The loss will have generated an impact that might be felt for a long time. The good news is that if you work to shore up your security after a failure, trust can be rebuilt. Rarely do companies go out of business for this kind of a security breach. If the information was of a personal nature, it may be more difficult for people to secure a new credit card, protect themselves from identity theft, or prevent bad actors from trying to steal money from their bank accounts.

Integrity loss

Whenever critical infrastructure has been compromised, whether it's a server or a network, it temporarily loses its ability to host services and data in a trusted manner. Luckily, this is the simplest problem of all to overcome.

Make sure you have applied all the security patches and increased security on the devices that were involved in the breach. Recover any lost data from backups. Monitor the regenerated system or systems like crazy. Be aware that some of the data that may have been compromised can contain information that makes it easier for a hacker to gain access to the newly regenerated system.

Data access loss

Many scenarios can lead to data loss. Data theft might have occurred, or data may have been encrypted during a ransomware attack, or the data storage device may have been attacked or simply failed. Part of the risk assessment must include the plan for dealing with these kinds of catastrophic losses and a plan to recover from them.

Data access loss can also be temporary, caused by network failure such as the one caused when the cloud computing company, Fastly, went down. That failure took down some of the largest Internet businesses for an hour in June of 2021.

Access to data can also be lost to a software failure such as the database management system's failure to respond or the hardware hosting the data failing or degrading. Hackers can also block access to data through exploits such as denial of service (DoS) attacks.

When you build the risk assessment database, you want to track fields such as these:

- The prospect that the negative event will occur
- The possibility of a confidentiality breach
- The impact of integrity loss
- The impact of loss of availability

With each of these items, you should include the *security level* (high, medium or low) and the *mitigation plan* — in other words, instructions for what to do when things go wrong and you haven't had your morning coffee yet.

TIP

The good news is that much of the hard work of developing a cloud security framework has already been done for you by somebody else. You can make free use of the following established frameworks:

- **NIST risk management framework:** `https://csrc.nist.gov/Projects/risk-management`
- **CSA CCM framework:** `https://cloudsecurityalliance.org/research/cloud-controls-matrix`
- **ISO 27017/18 framework:** `www.iso27001security.com/html/27017.html`
- **ISO 27701 framework:** `www.iso.org/standard/71670.html` (Privacy information management)

Avoiding Security Work with the Help of the Cloud

Using a cloud for your applications or data storage doesn't completely free you from the duties of cybersecurity, but it does move *some* of the responsibility to the cloud service provider. This section talks about what those responsibilities are and how you can best work with your cloud service provider to implement the best security plan.

Having someone else ensure physical security

Physical security in a data center can be a costly and time-consuming headache. Badges, biometrics, physical barriers, and closed circuit camera systems are all part of the physical security you may need to maintain around your server equipment. Okay, you might have your server in a repurposed utility closet with a cooling fan, but if you're serious about protecting direct access to the server, you need a great deal of infrastructure, continued maintenance, and personnel to manage it all.

By the way, that server running in the closet just may have data on it that you'd rather not let out into the wild. Part of the risk analysis will reveal just how much protection you should have around this device and deciding whether the data and applications should live in the cloud is part of that assessment.

One benefit of using the cloud for your services and data storage is that the cloud service provider is ultimately responsible for maintaining physical security around the hardware hosting your stuff.

Making sure providers have controls to separate customer data

Cloud service providers generally host many customers on the same hardware. This is known as multitenancy. When malware infects one tenant, it may allow access to the hypervisor that controls the virtual machines on the device, potentially allowing unauthorized access to other virtual machines belonging to other cloud customers. There is no simple fix other than to guard against malware. It's important to understand that multitenancy is one of the risks of doing business in the cloud.

Recognizing that cloud service providers can offer better security

Let me give you an example — here are some of the things Amazon Web Services does to guarantee the security of your applications and data:

- **Geographic site selection** to reduce risk from natural disasters such as earthquakes, hurricanes, and flooding
- **Multiple data centers** that provide a redundant backup and failover mechanism

- **Services** such as business continuity plans and pandemic responses
- **Restricting physical access** to approved employees and contractors
- **Monitoring and logging all data center access** as well as providing security guards, CCTV cameras, and sensor-intrusion detection systems
- **Monitoring data centers** for fire, water leaks, climate and temperature, and electric power with backup
- **Carrying out security and risk review** internally and by third-party companies to evaluate ongoing security risks

As you can see, these measures are more than most businesses — even large businesses — will want to take on by themselves. You literally rent all this security when you begin using a cloud service provider.

REMEMBER

These measures aren't unique to AWS. All major cloud service providers have these kinds of security measures in place. Some of them even surpass these measures with antipersonnel plants, such as creeping juniper and other noxious or thorny plants, around the building, antitank barriers that can be raised by security, and even oxygen-free server rooms.