
Growing Your
Business Securely
Colorado
SBDC
PIKES PEAK Small Business Development Center

Adding Employees Safely

- ✓ Human Resource Policies
  - ✓ Onboarding and Offboarding
  - ✓ Remote Work Policy
- ✓ Identity and Account Management
  - ✓ Principle of Least Privilege

- Background checks
- Signed policies
- Security training
- Immediate turning off of accounts at termination
- Return of all hardware/equipment prior to last check
- IAM
- Only give each person access to only what they need to complete their job. Admin for all might be easier to set up but allows for many more problems.
- If more than 2 computers to manage – find a centralized server system.

Security Policies that Make Sense

- ✓ Acceptable Use Policy
- ✓ Security Awareness Training Policy
- ✓ Disaster Recovery and Business Continuity
- ✓ Incident Response
- ✓ Identity Management
- ✓ Patch and Maintenance

All plans and policies must be reviewed at least once a year

Because acceptable use policies are intended to be read in full by each employee, they should be as concise as possible, only a few pages long at most. For increased readability, it's a good idea to take advantage of bullet points and numbered lists to stress the most important information.

Some of the key elements that no acceptable use policy should leave out are basic data security practices, such as the prohibition of sharing passwords via email and general restrictions covering various illegal activities

To deliver the biggest positive impact possible, security awareness training should encompass not just new hires but also existing employees who have been with the organization for some time. Simulated cyber attacks can then be used to reveal security gaps and provide employees with valuable practical experience

An identity management policy should cover not only authentication mechanisms but also password provisioning and employee offboarding. An entire section is typically dedicated to password requirements to ensure that all passwords are adequately strong and unique.

Disaster recovery and business continuity are two closely linked practices whose purpose is to prepare an organization for disruptive events, helping it resume operation as quickly and painlessly as possible. Besides cyber attacks, disruptive events also include internal emergencies such as loss of power and external emergencies such as floods and storms.

The content of a disaster recovery and business continuity policy should always reflect the unique business processes and IT resources of each organization, which is why performing a disaster recovery business impact analysis is a good first step. Once created, the policy should be thoroughly tested to verify that it fulfills its intended purpose.

Knowing that it's only a matter of time before a small business gets in the crosshairs of cybercriminals, it's paramount to establish an incident response policy and describe the processes and procedures necessary to detect, respond to, and recover from cybersecurity incidents.

Because all organizations deal with different cyber threats, their incident response policies must be created to reflect their unique needs while addressing the six key phases of an incident, as defined by the SANS Institute: preparation, identification, containment, eradication, recovery, and lessons learned.

A patch & maintenance policy specifies who is responsible for the discovery, installation, and testing of software patches and describes the conditions under which they are applied. It ensures that the right patches are applied at the right time by the right people.

For a patch & maintenance policy to be effective, it needs to encompass all IT assets that cybercriminals could exploit to infiltrate the target organization, including laptops, desktop computers, mobile devices, point-of-sale systems, servers, networking equipment, and all software running on these and other devices.

1.Install SSL – buying a simple Secure Sockets Layer certificate is a crucial first step.
2.Use anti-malware software – to scan for and prevent malicious attacks.
3.Make your passwords uncrackable – 123456 won't cut it!
4.Keep your website up to date – using out-of-date software is like leaving your back door unlocked.
5.Don't help the hackers – look out for phishing emails and other scams.
6.Manually accept on-site comments – keep control over potentially dodgy comments.
7.Run regular backups – to prepare for the worst case scenario.
8.Protect against cross-site scripting and injection attacks – understand what they are and how to protect yourself.
9.Implement web application firewalls – form a shield between your website and the internet.

So if you're not using a plugin, theme, or third party component — uninstall it. Especially if you're not keeping up with updates on your site. Keep only what you're actively using on your website. And remember: disabling a plugin or theme is not the same as removing it.
Here are some ways that you can enhance the security of your admin panel:
•Restrict access to specific IP addresses

•Require CAPTCHA
•Limit login attempts
•Use a non-standard URL

Applying these techniques to your admin pages can deter brute force and password guessing attempts, as well as limit access for bad actors.

nstead of “Your password is incorrect”, change failed password attempt messages to something like “Login credentials invalid.”

Logs are exceptionally valuable for website monitoring. They’re also very helpful when you need to troubleshoot technical issues or ensure user accountability. Furthermore, if you have an ecommerce website, logs are mandatory for PCI DSS compliance. And storing logs for future analysis is also a critical piece for GDPR, CIPA, and other regulations.

Securing Your Supply Chain

Supply chain security involves managing the risk of external suppliers, vendors, logistics, and transportation throughout a company's business operations. This applies to any entity or organization involved in the delivery of products or services.

- ✓ Know your data
- ✓ Conduct a supply chain security risk assessment
- ✓ Create a detailed security program
- ✓ Limit your suppliers' access to critical information and assets

A secure supply chain accurately identifies, analyzes, and mitigates any risks associated throughout an organization or third-party organizations.

✓Impersonating suppliers for fraud

✓Credential theft

✓Data theft

Sophisticated attacks known as business email compromise (BEC) sometimes involve fraudsters impersonating suppliers in order to trick a client into wiring them money. The attacker will usually hijack an email account belonging to one party or the other, monitoring email flows until the time is right to step in and send a fake invoice with altered bank details.

Attackers steal the logins of suppliers in an attempt to breach either the supplier or their clients (whose networks they may have access to). This is what happened in the massive Target breach of 2013 when hackers stole the credentials of one of the retailer's HVAC suppliers.

: Many suppliers store sensitive data on their clients, especially companies like law firms that are privy to intimate corporate secrets. They represent an attractive target for threat

actors looking for information they can monetize via extortion or other means.

Conduct a supply chain security risk assessment

Once you have an understanding of the sensitive data your business is storing, you can conduct a supply chain security risk assessment to determine what risks your business may be facing. This includes:

•Evaluating whether you need to keep sensitive data.
•Determining how data is currently stored.
•Looking at third-party access rights to data.
•Appraising partners for cybersecurity weaknesses.
•Assessing hardware and software for vulnerabilities.

Create a detailed security program

A security program is a document that outlines the policies, procedures, and tools your business will use to manage your supply chain risks. According to the FTC, an effective data security plan encompasses four elements: physical security, electronic security, employee training, and the security practices of third-party partners.

Develop an incident response plan

G Suite vs. Office 365 Security Features

Data Monitoring & Protection

Regarding data monitoring and protection, Google controls its entire hardware stack. It means that it can address and block security threats quickly. G Suite also offers full data encryption, while its machine learning capabilities help to detect threats more efficiently. When it comes to user data protection, G Suite focuses on malware threats in terms of infection prevention.

Office 365, on the other hand, offers an email filtering service that targets advanced spam and malware viruses. These include malicious URLs with various phishing traps and other similar infections. This platform is more focused on overall cloud security. Data encryption is also a top priority.

Compliance Management

Concerning compliance management, Google has strong user contracts that ensure their compliance environments are maintained.

That said, the platform is compliant with the following certifications:

•ISO 27001, 27018
•SOC 2, SOC 3
•COPPA
•HIPAA
•FERPA

•EU Data Protection Directive and GDPR

Office 365, on the other hand, has over 900 controls built in its compliance framework. It helps the platform stay on top of every development and industry compliance standards. Besides, a team of compliance specialists track all of these regulations and helps build them into their programs.

Office 365 compliance certifications:

•ISO 27001, 27018
•SOC1 Type II & SOC2 Type II
•SSAE16
•FISMA
•HIPAA
•EU Data Protection Directive and GDPR

User Access

G Suite had faced some challenges in the past since it had a minimal set of security management features. And even if it has made some strides more recently, companies should still review G Suite's user controls to make sure that it suits their respective industry. Nevertheless, admins can more easily manage user accounts, user permissions, and control access.

With Office 365, user control is built into every section. Admins have full control of security policies surrounding content sharing and external users. It allows them to create customized policy infrastructures with unique security demands based on their organization. If implemented correctly, this dramatically increases cloud security.

Automatic Updates

Regarding software and system updates, both the G Suite and Office 365 offer a seamless experience, automatically weeding out any weak security issues. Office 365 used to have a problem with this, but since it has become fully integrated into the cloud, this is no longer an issue.

Takeaway

When it comes to the bottom line, both the G Suite and Office 365 have well put together security infrastructures. And while both platforms can be useful for companies, there is one final point to consider - namely data privacy.

While Microsoft has made it clear that they will not scan user data and make it available to third parties for advertisement purposes, the same thing cannot be said about Google. And with Microsoft's years of experience in optimizing security strategies and patching up security vulnerabilities, it makes Office 365 a better candidate.

small businesses should consider several factors before subscribing to an MSP. For example, does an MSP fit in your budget? Do you need someone on-site who can fix problems like printer jams? Are you sure your technology is secure?

An MSP is a proactive solution. If an MSP operates effectively, it should prevent technical issues from occurring. It constantly monitors IT elements like hardware, applications, security, technology trends, and the internet and notifies you when there's an issue or abnormality. The MSP may recommend that you upgrade technology to boost productivity.

Ultimately, you're paying for someone to keep your business from having issues instead of fixing them.

MSPs offer business continuity. As a business owner, do you ponder how you would go about restoring all your systems and data in the event of a disaster? If not, you should. This is an area where an MSP can help you tremendously. A good MSP can create an efficient disaster recovery plan that will help you sleep at night, knowing that if disaster strikes, your business can endure it. This is particularly important as cybersecurity risks, such as ransomware attacks, become more prevalent.

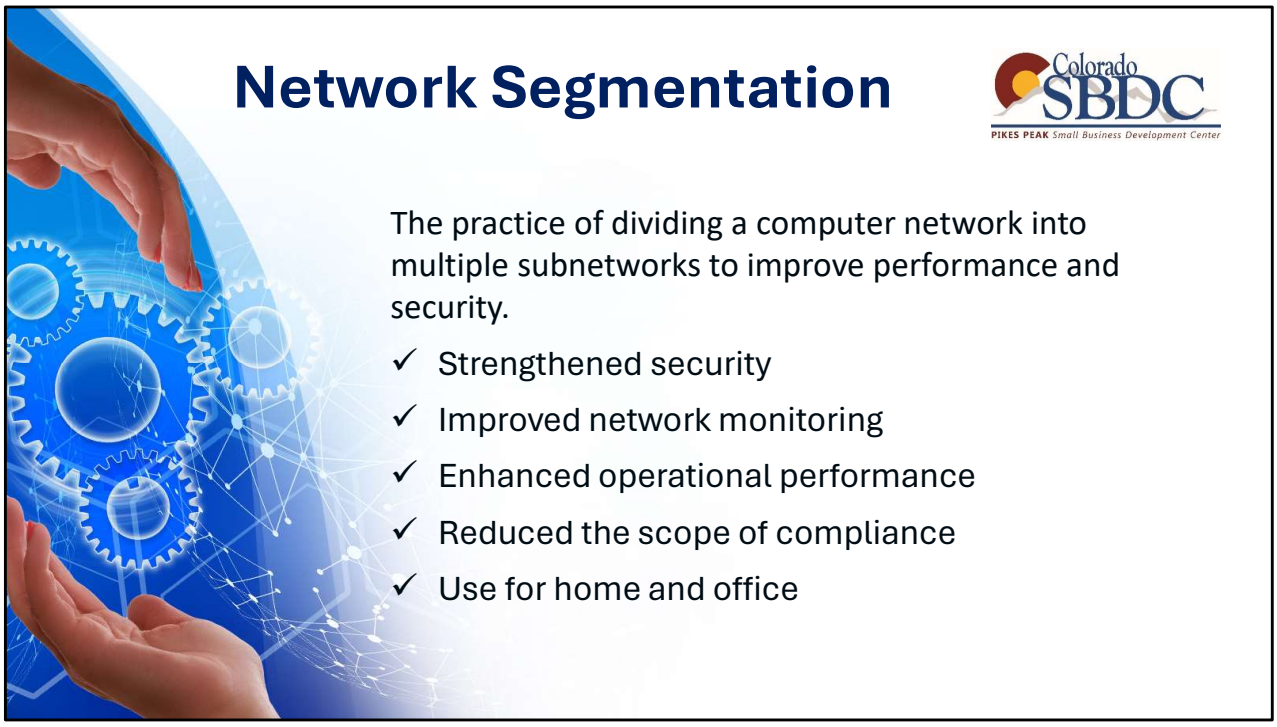
MSSP: **Managed firewall**: A managed firewall refers to a service that provides stronger threat management through the implementation of security experts. These professionals constantly monitor your firewall, as well as respond to potential threats. Using a managed firewall is similar to hiring a watchman, policeman, and detective all at the same time. Your system's network traffic is scrutinized to observe and track patterns. These patterns are used to form security parameters. When an event acts outside of these parameters, it triggers an alert and the potential threat is addressed.

1.Intrusion detection: Traditionally, networks are often compared to castles. A big enough moat, theoretically, will protect everything you value on the inside. However, modern intrusion detection involves second-guessing all components, people, and software, whether they are inside or outside the "castle." Intrusion detection by a capable MSSP involves protecting all devices and systems, as well as making sure they are not used by bad actors to harm other systems inside—or outside—your organization.

2.Virtual private network (VPN): In the hands of an MSSP, a VPN can be configured to securely shelter your organization's operations. Because it is shielded from intrusion by other users, a private VPN minimizes the attack surface significantly. If only necessary users are granted access to the VPN, your MSSP only has to implement security measures to safeguard the network from those users and their devices.

3.Vulnerability scanning: While identifying potential threats is an essential step, an MSSP also scans for vulnerabilities in your network. Sometimes, these include obvious targets for cyber criminals, such as workspaces and sensitive data. In other cases, areas or systems that criminals want to access can be penetrated using a vulnerability two or three degrees removed from it. An MSSP can pinpoint each vulnerability, whether it is inside an attack surface, adjacent to it, or a few degrees away.

4.Antiviral services: The diversity of viral attacks climbs every year, and it is often difficult for IT teams to keep up with the expanding selection of threats. An MSSP has the resources to hone in on the viruses that pose the most imminent threat to your network and its users. The MSSP can then design a portfolio of antiviral services that takes aim at the most salient threats. In addition, general antiviral measures can be implemented at various levels and locations within the network. For example, antiviral solutions can be arranged to meet the protection needs of in-house servers, while different solutions can be designed for cloud servers.



•**Strengthened security.** Network segmentation minimizes security risks by creating a multi-layer attack surface that prevents lateral network attacks. As a result, even if attackers breach your first perimeter of defense, they are contained within the network segment they access.

Improved network monitoring. Dividing your network into organized segments makes it easier to isolate incidents and quickly identify threats.

Enhanced operational performance. Traffic is limited to specific zones based on need. This reduces the number of hosts and users within any given subnet, decreasing congestion and boosting performance across the board.

Reduced the scope of compliance. Segmentation allows you to separate regulated data from your other systems, making it easier to manage compliance and apply policies with a targeted approach.

Thank you

- For more information:
- Nina Amey
- Cybersecurity Program Manager
- Pikes Peak SBDC
- nina@pikespeaksbdc.org

Colorado SBDC
PIKES PEAK Small Business Development Center