

Top 10 Security Best Practices for Small Business



Check Point
SOFTWARE TECHNOLOGIES LTD.





Check Point
SOFTWARE TECHNOLOGIES LTD.

SMALL BUSINESS NEEDS **SECURITY** TOO



What Are The Top 10 Security Best Practices for Small Business?

Why Are Small Businesses Targeted?

83% of SMB security incidents
result in a confirmed data breach

— Verizon DBIR 2015



LARGE BUSINESS

Significant people
and budget for
high levels
of protection



SMALL & MEDIUM BUSINESS

Valuable information
but weaker protection:
Less people and less
investment in security

Why Not Focus on Security?

Too small to be a target?

Believe they have sufficient protection in place?

Perception that cyber security is too expensive and complex?

A **failure** to protect against cyber threats could actually cause your business to suddenly be **out of business**.

Top Security Best Practice #2



#2: Secure Every Entrance

All it takes is one open door to allow a cybercriminal to enter your network. Just like you secure your home by locking the front door, the back door and all the windows, think about protecting your network in the same way.

Consider all the ways someone could enter your network, then ensure that only authorized users can do so.

- Ensure strong passwords on laptops, smartphones, tablets, and WIFI access points.
- Use a Firewall with Threat Prevention to protect access to your network (like the Check Point 700 Appliance).
- Secure your endpoints (laptops, desktops) with security software such as Anti-virus, Anti-SPAM and Anti-Phishing.
- Protect from a common attack method by instructing employees not to plug in unknown USB devices.

Top Security Best Practice #3



#3: Segment Your Network

A way to protect your network is to separate your network into zones and protect the zones appropriately. One zone may be for critical work only, where another may be a guest zone where customers can surf the internet, but not access your work network.

Segment your network and place more rigid security requirements where needed.

- Public facing web servers should not be allowed to access your internal network.
- You may allow guest access, but do not allow guests on your internal network.
- Consider separating your network according to various business functions (customer records, Finance, general employees).

Top Security Best Practice #4



Check Point
SOFTWARE TECHNOLOGIES LTD



#4: Define, Educate and Enforce Policy

Actually HAVE a security policy (many small businesses don't) and use your Threat Prevention device to its full capacity. Spend some time thinking about what applications you want to allow in your network and what apps you do NOT want to run in your network. Educate your employees on acceptable use of the company network. Make it official. Then enforce it where you can. Monitor for policy violations and excessive bandwidth use.

- Set up an Appropriate Use Policy for allowed/disallowed apps and websites.
- Do not allow risky applications such as Bit Torrent or other Peer-to-Peer file sharing applications, which are a very common methods of distributing malicious software.
- Block TOR and other anonymizers that seek to hide behavior or circumvent security.
- Think about Social Media while developing policy.

Top Security Best Practice #5



#5: Be Socially Aware

Social media sites are a gold mine for cybercriminals looking to gain information on people, improving their success rate for attacks. Attacks such as phishing, spearphishing or social engineering all start with collecting personal data on individuals.

- Educate employees to be cautious with sharing on social media sites, even in their personal accounts.
- Let users know that cybercriminals build profiles of company employees to make phishing and social engineering attacks more successful.
- Train employees on privacy settings on social media sites to protect their personal information.
- Users should be careful of what they share, since cybercriminals could guess security answers (such as your dog's name) to reset passwords and gain access to accounts.

Top Security Best Practice #7



#7: Maintain Your Network Like Your Car

Your network, and all its connected components, should run like a well oiled machine. Regular maintenance will ensure it continues to roll along at peak performance and hit few speed bumps.

- Ensure operating systems of laptops and servers are updated (Windows Update is turned on for all Systems).
- Uninstall software that isn't needed so you don't have to check for regular updates (e.g., Java).
- Update browser, Flash, Adobe and applications on your servers and laptops.
- Turn on automatic updates where available: Windows, Chrome, Firefox, Adobe.
- Use an Intrusion Prevention System (IPS) device like the Check Point 700 Appliance to prevent attacks on non-updated laptops.

Top Security Best Practice #8



#8: Cloud Caution

Cloud storage and applications are all the rage, but be cautious. Any content that is moved to the cloud is no longer in your control. And cybercriminals are taking advantage of weaker security of some Cloud providers.

- When using the Cloud, assume content sent is no longer private.
- Encrypt content before sending (including system backups).
- Check the security of your Cloud provider.
- Don't use the same password everywhere, especially Cloud passwords.

Top Security Best Practice #9



#9: Don't Let Everyone Administrate

Laptops can be accessed via user accounts or administrative accounts. Administrative access allows users much more freedom and power on their laptops, but that power moves to the cybercriminal if the administrator account is hacked.

- Don't allow employees to use a Windows account with Administrator privileges for day-to-day activities.
- Limiting employees to User Account access reduces the ability for malicious software (better known as malware) to do extensive damage at the "administrator" privileged level.
- Make it a habit to change default passwords on all devices, including laptops, servers, routers, gateways and network printers.

Top Security Best Practice #10



Check Point
SOFTWARE TECHNOLOGIES LTD



#10: Address the BYOD Elephant in the Room

Start with creating a Bring-Your-Own-Device policy. Many companies have avoided the topic, but it's a trend that continues to push forward. Don't avoid the elephant in the room! It comes back to educating the user.

- Consider allowing only guest access (internet only) for employee owned devices.
- Enforce password locks on user owned devices.
- Access sensitive information only through encrypted VPN.
- Don't allow storage of sensitive information on personal devices (such as customer contacts or credit card information).
- Have a plan if an employee loses their device.

Check Point Is The Clear Choice

NETWORKWORLD®
2013 and 2014 **WINNER**
Best Small Business Security
UTM Devices

2 YEARS in
a ROW!

Protect Your Small Business with the Clear Choice

Network World compared security gateway products on the market and chose the Check Point as the Clear Choice to protect small businesses.

“Check Point is our Clear Choice Test winner... It has an appealing user interface, a lot of great security features, and is simple to manage and create new security rules.”

— Network World

SCORECARD

Product	Calyptix	Check Point Software	Dell/ Sonicwall	Fortinet	Sophos	WatchGuard
Installation	3.5	5	3.5	3	3	5
Features	3.5	4.5	4	4.5	4	4.5
Value	3.5	5	3	4	4	5
Total	3.5	4.8	3.5	3.8	3.7	4.8

SCORING KEY > 5: Exceptional, 4: Very Good, 3: Average, 2: Below Average, 1: Consistently Subpar