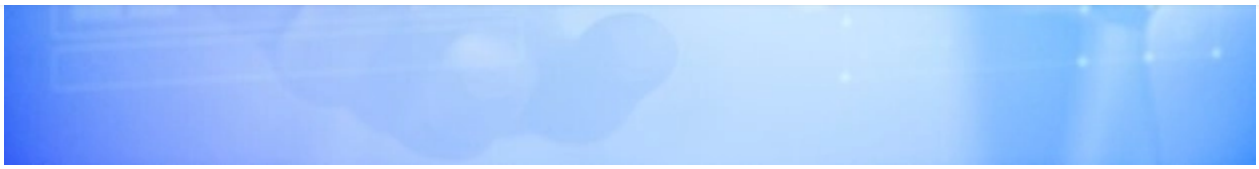
powerconsulting
technology for people

...

# Full Checklist for Cyber Security Assessments

Cyber Security
November 18, 2019

powerconsulting
technology for people



## Are you in denial about cybersecurity?

If you think you aren't because your business is too small or doesn't have worthwhile data to steal, think again. Hackers know that information systems for small and medium businesses (SMBs) typically have weak security and are easy to exploit. Consider these statistics:

- Almost half (49%) of SMBs report that cyber breaches could cost them $100,000 or more, and 20% say that breaches could cost $1 million to $2.5 million.
- An astonishing 60% of SMBs that are hit with cyberattacks never recover and end up closing down.

It is nearly 100% certain that your business will be victimized by a cyberattack; it's a question of when, not if. Considering the damage a cyberattack can wreak on your business, you can't remain in denial any longer. The time to assess your cybersecurity preparedness is now.

powerconsulting
technology for people

# Cyber Security Risk Assessment Checklist

To that end, we've provided the following comprehensive cybersecurity risk assessment checklist of actions to take to

- Assess your risk,
- Identify security threats,
- Reduce your vulnerability, and
- Increase your preparedness

For that eventual hack that does penetrate your defenses.

The government of Utah provides a massive 57 point audit checklist – linked here – but it doesn't give businesses a quick and easy way to hone in on the areas that actually secure a business.

To that end, we created this checklist for a security audit that will provide you with the security controls and incident response you need.

If you're unsure about your own cyber security, Click Here to get a free cyber security audit from Power Consulting NYC Managed IT Services provider.

operate. Important things to cover includes phishing, password security, device security, and physical device security.

Employees need to know what potential cyber security breaches look like, how to protect confidential data and the importance of having strong passwords.

It's recommended to have organizational workshops with your company at least once every six months.

## 2. OS and Application patches and updates:

The single most important—and simplest—action you can take is keeping your computers' applications and operating systems up to date with the latest security patches. If your computers are still running on Windows XP, you are at risk: Microsoft stopped supporting this version of Windows long ago, and is no longer providing security updates. The venerable Windows 7 will soon suffer the same fate. If you do nothing else, at least update your systems with the latest versions and security patches.

## 3. Antivirus updates:

Simply having an antivirus application is not enough—it has to be

Make sure all your passwords are changed from their defaults and are not easy to guess ("password," "admin," and "1234" are poor choices). Where possible, implement multi-factor authentication to further increase security.

## 5. Access control measures:

All users should have only the minimum data access required to do their jobs. When every user has access to sensitive data, accidental or deliberate exposure or release of the data can occur, leading to damaging consequences. Consider keeping highly sensitive systems under physical lock and key in addition to password protection.

## 6. Minimize administrative access:

Similarly, most users should not have administrative access to computers, networks, or applications.Limiting this access can prevent users from installing malware or accidentally turning off security measures.

Least privilege is the practice of preventing certain users from accessing certain computer processes and data by restricting their access. Typically, their are "super user" or "standard user" accounts

ensure that the most sensitive and confidential data is not accessed.

Together you will create a secure network architecture.

## 8. Device security:

Implement disk encryption and remote-wipe capability on all company devices to render them useless if they are lost or stolen. Establish a strong, sensible policy regarding the use of personal devices for work (known as “bring your own device,” or BYOD).

## 9. Protect mobile devices:

Company-owned and personal mobile devices should be protected with strong screen locks or biometric authentication as well as remote-wipe capability. Establish and enforce no-nonsense organizational policies around the use of mobile devices.

## 10. Secure communications:

Set up email encryption on your email applications and train your staff on how to use it. Never use email to share sensitive data, and avoid using devices outside the company’s control for email.

## 12. Staff training on cybersecurity awareness and policies:

Humans are the weakest link in any security scheme. Keep your staff vigilant with periodic training on your IT policies as well as how to spot cyber threats such as phishing.

## 13. Properly configured layered and configuration security:

Layered security is implemented by having layers of security that provides different levels of protection. It's essential for your organization to use some type of layered security, such as a firewall to protect against cyber attacks.

As a best practice, it's important to have anti-virus/malware software in place, a fire wall, and lastly an intrusion prevention system (IPS).

The implementation of  layered security can be tricky, and it's best to engage with an expert before deployment.

Internally these scans detect if there was harmful programs downloaded onto a computer. Or externally detect the strength of the network segmentation and segregation.

## 15. Data backups:

Regularly backing up your data to a secure, encrypted, and off-site location can aid in recovery from a cyberattack as well as other human and natural disasters. It's also essential for compliance with certain government regulations.

## 16. Cyberattack response planning:

A cybersecurity breach response plan is a regulatory requirement in several industries. Furthermore, it identifies a clear path of what to do to mitigate the damage from a successful cyberattack and how to get your systems up and running immediately. Defined escalation levels cater to auditor and regulatory requirements.

## 17. Cybersecurity insurance:

This is a prudent investment to cover financial losses in the event of a

inexpensive, but its cost pales in comparison with that of a successful cyberattack.

If you don't have the expertise to implement these measures yourself, find a reputable, experienced cyber security service provider to do it for you. It can mean the difference between success and failure of your business.

**Chris Power** / About Author

› More posts by Chris Power

powerconsulting
technology for people

Full Name*

Company Email*

Type your company email

Phone number*

Describe your IT Needs

powerconsulting
technology for people

Please verify your request*

I'm not a robot

reCAPTCHA
Privacy - Terms

Request a Proposal

Google Rating
4.5