INTEGRITY
TECHNOLOGY SOLUTIONS

Data Security Checklist:

20 Ways to Keep Hackers Out and Protect Your Company

TABLE OF CONTENTS

INTRODUCTION

Each year, cybersecurity incidents continue to increase.

This is especially dangerous as many businesses store personally identifiable information, protected health information, or other sensitive data.

The proper controls must be put in place to safeguard this information.

That's why many businesses are looking ahead to bolster their existing security posture.

In fact, 71% of businesses planned to increase their security spending over the next three years, according to the Kaspersky Global Corporate IT Security Risks Survey[1].

Chances are your business would benefit from assessing your security posture, as well. With this 20-point checklist that covers topics related to software updates, cloud strategy, and more, you'll be able to see where your organization excels and where you may need to fill the gaps.

[1] https://usa.kaspersky.com/blog/it-security-economics-2020-main/23401/

DATA SECURITY CHECKLIST

Use this checklist to assess your organization's security posture.

☐ 1. ALWAYS USE UNIQUE AND COMPLEX PASSWORDS

Using a password manager can help generate and keep track of credentials. Just be sure that your master password can't be guessed. Passphrases will minimize the likelihood your accounts can be accessed. Be sure you have policies in place to change passwords and passphrases multiple times per year.

☐ 2. ENCRYPT EVERYTHING

Hackers and cybercriminals continually get more creative in stealing data. Using encryption can help foil their plans.

☐ 3. MONITOR YOUR NETWORK FOR SUSPICIOUS OR UNAUTHORIZED ACTIVITY

Hackers are vigilant, so businesses must be, too. Actively monitoring your network can help catch bad actors before they steal sensitive data or hold your data hostage. Many businesses have monitoring in place, but it may not be at the appropriate level for yours.

☐ 4. ENABLE MFA FOR REMOTE ACCESS

Now that business data can be accessed anywhere, your business must require your employees to use multifactor authentication (MFA). Sometimes referred to as two-factor authentication (2FA), this control requires more than just a password to ensure the user logging in is the person that's supposed to be there. Facial or fingerprint recognition and temporary codes are examples of multi-factor authentication.

☐ 5. TEST FOR SYSTEM VULNERABILITIES

What you don't know can hurt you when it comes to data security. Even if you feel that your data is safe, test it. Try to get past your own defenses. If vulnerabilities exist, either your organization or the partner you hire to help should be the one to find them.

☐ 6. INSTALL SOFTWARE UPDATES AS THEY'RE MADE AVAILABLE

Software updates often contain security patches against known threats. Keeping your organization's software up to date is critical in preventing attacks.

☐ 7. BACKUP AND CONDUCT RESTORE TESTING OF YOUR DATA REGULARLY

Backing up data is an important facet of any security strategy. In the event of a cyber attack, a natural disaster, or other large-scale emergency, having a backup policy in place saves and restores data.

☐ 8. HAVE AN INCIDENT RESPONSE PLAN IN PLACE

When your business suffers an attack or is compromised, time is of the essence—especially if lives are at risk. Know who will be involved in the process and what steps to take to safely restore your network and data assets as quickly as possible.

☐ 9. HAVE A CLOUD STRATEGY

The cloud gives businesses enormous storage and application capabilities without the logistics and cost attached to prior methods. But, the cloud requires diligent data security measures. Before storing or transacting important data in the cloud, find out how to keep it safe.

☐ 10. IMPLEMENT MULTI-LAYERED SECURITY

Using a multi-step verification process and other multi-layered security measures makes your business a less-appealing target and slows hackers down.

☐ 11. BE WARY OF SHARING YOUR MOBILE DEVICE

Smartphones, tablets, and more can give cybercriminals access to business data. Use a password-protected lock screen and other features to ward off hackers. In general, be wary of who is using your mobile device.

☐ 12. EDUCATE YOUR STAFF ABOUT SECURITY AWARENESS

One of the best ways to prevent a data security issue is training your staff to be prepared for it. In your security awareness program, review best practices, policies, and standards for protecting your business. Communicate the current threat landscape and how to report suspicious activity.

☐ 13. DON'T EMAIL SENSITIVE INFORMATION

Email is a vulnerable communication method that can easily be accessed. If employees are discussing or sharing sensitive data over email, they're putting the company at risk. Encrypted email can mitigate this risk.

☐ 14. MOVE FROM ANTIVIRUS TO A NEXT-GENERATION EDR SOLUTION

Legacy methods of antivirus are no longer an effective way to protect against current threats. Next-generation endpoint detection and response (EDR) solutions can help protect against common threats like ransomware and malware.

☐ 15. UPDATE YOUR BROWSER

Web browser updates often strengthen the security of that browser. The more secure the browser, the more secure your data will be.

☐ 16. DEVELOP A SOCIAL MEDIA POLICY

Social media is a highly visible and easy platform on which to jeopardize company data. Train employees to be careful with their activity and what they're sharing on each platform.

☐ 17. CONTROL ACCESS TO COMPUTERS & DEVICES

Develop and maintain a standard for granting conditional access to sensitive data. Keep authentication standards high and keep data protected as much as possible.

☐ 18. IMPLEMENT PHYSICAL CONTROLS

If there are physical copies of sensitive data created, know where those copies are and where they'll end up. Consider adding security cameras, locks, security guards, or biometric controls to protect your data.

☐ 19. USE THE LOWEST ROLE POSSIBLE TO ACCESS WHAT YOU NEED

Keep data security by providing administrator role access only when necessary, and give most users less-expansive roles whenever possible.

☐ 20. SECURE YOUR WI-FI NETWORK

Protect your Wi-Fi network with a strong password or passphrase to keep unwanted guests out.

CONCLUSION

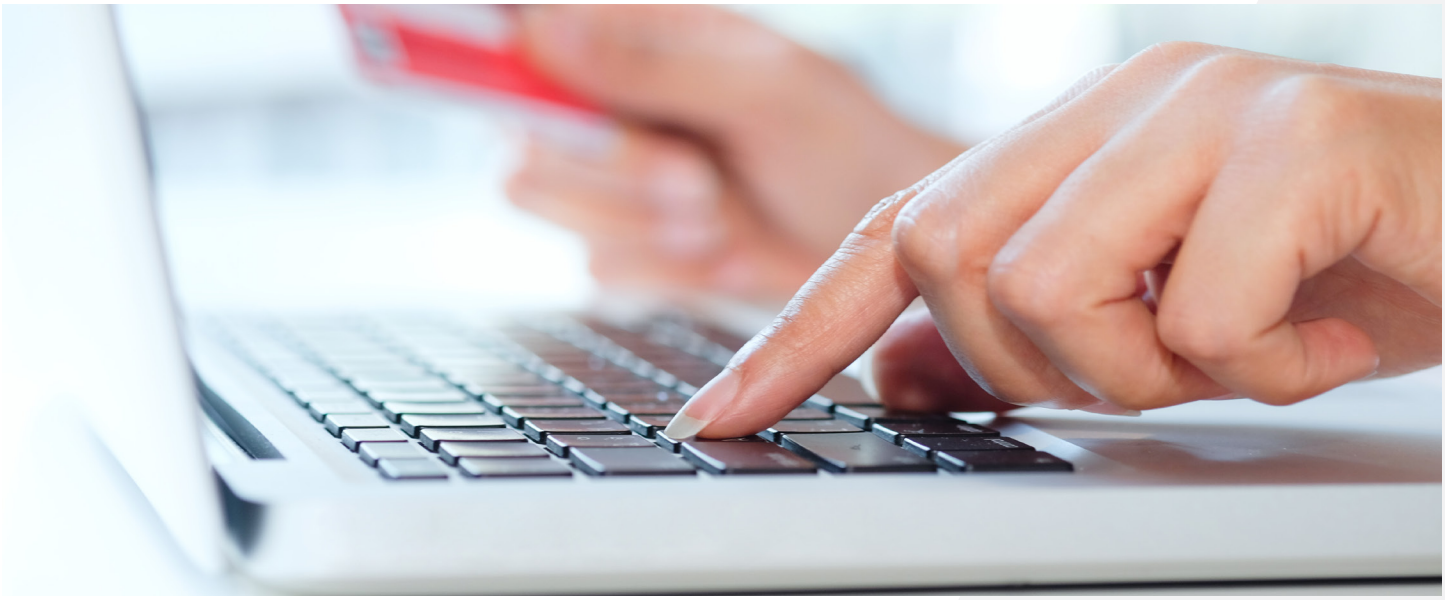
Protecting your organization is critical as cybersecurity threats increase. Whether you must meet compliance requirements or you just want to protect otherwise sensitive information, this checklist will help make sure your data is secure.

After you work your way through the checklist, see whether any controls listed are not enacted. Then, draft a plan to address those.

If you'd like assistance in securing your organization's data, please contact us at Integrity Technology Solutions.

309-662-7723

REQUEST A CONSULTATION



INTEGRITY
TECHNOLOGY SOLUTIONS

ABOUT

Founded in 1993, Integrity is a managed security service provider, offering community banks, clinical healthcare organizations, and small businesses end-to-end protection from cybersecurity threats. Integrity brings compliance and security expertise to its partners, keeping them in front of an ever-evolving technology landscape. Integrity serves as a full IT department for smaller businesses and a supplemental solution for larger organizations in need of IT and security assistance.

SERVICES

- IT Support, Planning, Consulting, and Compliance
- Managed IT Security Services
- Network Management
- IT Project Management & Implementation
- Data Backup & Disaster Recovery
- IT Vulnerability & Risk Assessments
- Cloud Services *(including Microsoft 365 and Azure Hosting)*
- IT Security Protection – Detection – Response
- Security Information and Event Management (SIEM)
- 24x7x365 Domestic Security Operations Center (SOC)
- Security Awareness Program