14 STEPS TO PROTECT YOUR ORGANIZATION

Protecting your organization from ever-evolving information security threats.

Administrative // Physical // Internal // External

TECH || INNOVATION
by BerganKDV

PROTECTING YOUR ORGANIZATION

1

CONDUCT A SECURITY ASSESSMENT

A well rounded information security approach starts with an comprehensive professional assessment to identify weak points and form an action plan. Through our vendor partnerships, our clients have access to free self-assessment tools that provide an overview of risks.

2

SPAM EMAIL CONTROLS

Evaluate tools available to your business to instantly remove phishing and dangerous emails before they even hit your inbox.

3

PASSWORD PROTECT

A good place to start is enforcing a policy that requires complex passwords and use a password manager to centralize and make it easier for your users.

4

SECURITY AWARENESS & TRAINING

Most problems are caused by users not having adequate training and following safe protocols. Measure your employee's success with frequent phishing and actionable training on information safety and security.

5

ENDPOINT SECURITY

Laptops, desktops and mobile devices. They can all be entry points for attacks. Mobile devices are used to conduct business daily, ensure your security protocols include all devices.

6

MULTI-FACTOR AUTHENTICATION

Even the most complex passwords are proven unsafe. Multi-factor authentication (MFA) is the act of adding an additional layer of security to an account to ensure only authorized users gain entry. We recommend enabling MFA on EVERYTHING or switching to programs that support MFA.

7

COMPUTER UPDATES

Automate software and updates. This will help ensure you have the latest security controls in place at all time. Use a third party tool to check quarterly.

8

DARK WEB RESEARCH

Think of this as the black market of the internet. Be proactive and know if your credentials or data is being sold online.

bergankDV

PROTECTING YOUR ORGANIZATION

9 **NEXT GENERATION FIREWALLS**
Ensure all of the features including DPI SSL are enabled, optimized and reviewed.

10 **ENCRYPTION**
Encrypting data that is in transit or at rest. To ensure it is adopted internally, you have to make it user-friendly and intuitive. Ensure the tool you implement is the right one for your organization.

11 **BACKUPS**
Testing your backup solution after a disaster is obviously not a best practice. Most SMB's don't have a documented data retention plan or test.

12 **CYBERINSURANCE LEGAL COUNSEL**
Know your policy and do your due diligence so that if a disaster happens you are covered.

13 **INCIDENT RESPONSE PLAN**
Are the critical teams in your organization on the same page for the procedure should a cyberattack or breach happen? Ensure your plan is appropriate and test.

14 **SECURING YOUR REMOTE WORKFORCE**
Make sure that your security posture doesn't forget about people working from home.

info@bergankdv.com // bergankdv.com // 1-866-400-6426

bergankDV