protectnow

Robert Siciliano CEO, CSP, CSI, CITRMS
Robert@ProtectNowLLC.com
Ph. 617-257-1870
Web: Https:/ProtectNowllc.com
Twitter: @ProtectNowLLC
Facebook: @CSIProtectionCertification

15 Actionable Fundamentals of Data Protection

1. **Have a Plan:** As the saying goes, “if you fail to plan, then you plan to fail”. But when it comes to data security “if you fail to plan, you plan to pay”. And that means you’re paying the bad guy or lawyers or the government in fines. Or you’re losing business because of a poor security reputation.
2. **Social Engineering:** Know that every time the phone rings, an email comes in, or even an invoice via the US Postal Service is received, that the communication could be designed to socially engineer or influence you or a staff member to transfer money out of your bank account for one reason or the other. No matter the reason for the communication, it’s intensity, immediacy or threating nature, the upmost scrutiny needs to be given before monies are paid. Just stop and think before taking action.
3. **Security Awareness Training:** Whether it be hardware, software, or human hacking, there are always vulnerabilities in all systems, all around us. The only way to properly plug these various holes is through education both in person, virtually, and through phishing simulation training. This requires a little bit of time and expense and is an absolute necessity of doing business in 2020 and beyond.
4. **Hardware:** Make sure your devices such as PC’s, laptops, mobiles, modems, routers and any peripherals are newer. Old hardware (5+ years) sometimes lacks internal resources to run current more secure software and firmware.
5. **Secure Software:** Keep all devices operating systems updated with the latest software updates and critical security patches. Install and run a paid version of antivirus, anti-spyware, anti-phishing and a 2-way firewall.
6. **WiFi Security:** Set up a secure WiFi connection in your home or business.
7. **VPN:** Ensure your laptop and mobile devices and its data are protected on open free WiFi by using a VPN or “virtual private network”
8. **Encryption:** Protect your data with encryption software.
9. **Tracking:** Install, set up and enable tracking software for lost or stolen laptops and mobile phones
10. **Backup:** Back up and sync all your information on redundant internal and external local hard drives. Back up externally to cloud based backup sites. Back up all data on iPhone and Android mobiles.
11. **Passwords:** Set up and run password manager software and eliminate password re-use by having a different password for every online account.
12. **Two Factor:** Set up two-factor or two step authentication for any and all critical accounts that deploy it.
13. **Social Engineering:** Recognize social engineering scams every time the phone rings, an email comes in or someone knocks on the door.
14. **IT Vendors:** Use your circle of influence or trusted network to make recommendations when hiring IT security contractors such as virtual Chief Information Security Officers (vCISO), or depending on the size and scope of the organization a Managed Security Service Provider also known as in MSSP to ensure the security of your network.
15. **Social media:** What you say, post, like, or share has repercussions. Manage your online reputation.