Information Security Basics for Independent Consultants

The average cost of a breach exceeds what the average consultant earns in a year. Protect your business and reputation by following these inexpensive security basics.

1. Back Up Your Data

2. Know Your Legal Obligations

3. Take Awareness Training
start-training.alfizo.com

4. Have E-mail Security

5. Follow Good Authentication Practices

6. Use Anti-Malware Software

7. Use Secure Wi-Fi

8. Update and Patch

9. Secure Mobile Devices

10. Use Encryption

11. Secure Assets on the Internet

P(WERS
EMERGING RISKS DIVISION

12. Buy Cyber Insurance

Alfizo®
Protecting Businesses from Cyber Threats
Alfizo.com

Gary Chan
Information Security Consultant
gchan@alfizo.com
929-525-3496

JD Powers
President
jdp@powersinsurance.com
314-333-4909

POWERS®
INSURANCE & RISK MANAGEMENT
PowersInsurance.com

Information Security Basics for Independent Consultants

Every business faces different security risks, so there is no one-size fits all security solution. This is a list of 12 activities that solo independent consultants should follow. Companies with multiple people or which store particularly sensitive information will likely need to do more than the activities described herein.

1. Back up your data: Save at least 6 months' worth of history, not just the last version. That way, if you get hit by ransomware, you can restore your data to pre-crisis times.

2. Know your legal, regulatory, and contractual obligations: More clients are inserting information security clauses into their contracts. Fortunately, most of those requirements will likely be satisfied by this guide.

3. Take awareness training: Watch security awareness videos to learn about general safety practices as individuals. Sign up for free videos here: https://start-training.alfizo.com

4. Have e-mail security: Use a commercial e-mail security solution to quarantine malicious e-mail and spam. Free versions come with most e-mail services, and you can purchase higher quality solutions for a modest monthly fee.

5. Follow good authentication practices: Multi-factor authentication makes it substantially harder for hackers to break into your account. Single sign-on solutions, like https://www.appsco.com/ , reduce the number of times you need to enter your password, meaning you're less likely to write your passwords down, making you more secure. If you must write your passwords down, then store your passwords in a digital vault.

6. Use anti-malware software: If you are on a budget, use the built-in Windows Defender for Windows and XProtect for Macs. If you can afford it, purchase higher-end software to better protect against the latest threats, like ransomware.

7. Use Secure Wi-Fi: If you own the Wi-Fi infrastructure, use a good password and the WPA2 protocol. Place all guests and customers on a separate guest network. Use VPN when on someone else's WiFi. Remember that everyone who knows the WiFi password can potentially see your data. If you travel heavily, use your own mobile hotspot.

8. Update and patch: Update and patch your operating system and applications frequently.

9. Secure mobile devices: Lock your devices when you are not using them. Have a way to remotely wipe mobile devices in case they are lost or stolen.

10. Use encryption: Encrypt everything that you don't consider to be public information.

11. Secure assets on the Internet: If you have a website, share files in the cloud, or have any other data on the Internet, be sure to follow instructions specific to the applications you are using to secure your data. If you have a contact form and get a ton of SPAM, consider adding a firewall and contact form filter.

12. Buy cyber insurance: Invest in an insurance plan to protect your business against unexpected events. Talk with a Powers insurance agent (https://www.powersinsurance.com/).

Do it yourself to save money, or accelerate your security program by hiring an information security specialist.

About Author: Gary S. Chan helps businesses achieve their security goals through his company Alfizo LLC, https://www.alfizo.com/ . Amongst many projects, Gary has architected anti-fraud systems for state agencies, built and managed the information security teams for an $11B+ company, led a 200-person organization that supports law enforcement, works as an independent security consultant, speaks at events, and is an evaluator and mentor for cybersecurity start-ups. He has multiple security certifications, including a CISSP, ISSMP, and CFE, and holds a degree in Electrical Engineering & Computer Science from MIT. Contact Gary: 929-525-3496, consultant@alfizo.com