CYBER SECURITY

Your company receives a statement from its credit card issuer that includes thousands of dollars in fraudulent charges. You return from a long weekend to find that your corporate network has been breached and all of your customer information, including credit card numbers and billing addresses, has been stolen. You receive an email from your bank telling you that your bank account has been accessed by a new device and asking you to navigate to a provided link and confirm the account's details.

These are not remote risks. All of these events happen thousands of times every day, and to businesses large and small. Cybercrime is by some measures the fastest growing type of crime and its costs are expected to reach $2.1 trillion by 2019.

Protecting you data and information systems has never been more important. Every computer and mobile device can be vulnerable to attack, and the consequences of such an attack can range from simple inconvenience to financial catastrophe. Depending on the particular industry, and the size and scope of the business, cyber security can be very complicated and may require specialized expertise. However, even the smallest business can be better prepared.

Contact Information
Reporting Claims or Loss
24-hour toll free number:
1.800.690.5520
Email to:
riskengineering@cfins.com

Cyber Security

Risk Management

C&F RISK ENGINEERS UNDERSTAND YOUR BUSINESS

Since 1822, Crum & Forster has successfully anticipated what's next. Our insurance policy is our promise to help you – the policyholder – in the event of a loss. It gives you a future benefit that you can count on. But C&F offers something more. Our Risk Engineers can help your operation right now.

Before you ever encounter a claim, our Risk Engineers can meet you and identify actual and potential loss sources. We'll conduct a thorough study of your company that includes exposures, hazards and accident trends. Together we'll review your current loss prevention efforts, physical location, loss information and other business records to pinpoint fundamental loss causes. Then we'll create an action plan with practical recommendations to strengthen existing safety programs. We can maintain an ongoing review of it to evaluate progress and effectiveness. We can even conduct a legal exposure review of your company's agreements. Everything we do is aimed at putting into place an effective loss control strategy that works consistently over time to lower your operation's risk of loss.

Our highly specialized Risk Engineers are strategically located throughout the country and have the experience, training and professionalism to provide risk management solutions to meet your business needs and contribute to your success. They have on average more than 20 years industry experience, many with roles dedicated to safety and training. And we invest not only in our insureds, but in the industry. We are members of and participate in many state associations and regularly present at industry conventions and events. These connections and experience are invaluable, and are key in assisting you in developing and deploying a modern, up-to-date safety and training program.

Our solutions are both innovative and established. Whether it's Accident Event Recorders (AERs) to help identify vehicle accident causes and tailor safety training, digital tracking systems, or online video training to assure OSHA compliance, we bring you the latest technology. Matched with the experience of our Risk Engineers, your operation benefits from the engineering awareness built over a lifetime and cutting edge safety science.

Start with the following simple steps, which are recommended by US-CERT, a partnership between the U. S. Department of Homeland Security (DHS) and the public and private sectors:

Use anti-virus software and keep it up-to-date.

- Activate the software's auto-update feature to ensure your software is always up-to-date.

Do not open e-mail from unknown sources.

- Whether they are from a known source or not, be suspicious of unexpected e-mails that include attachments.
- When in doubt, delete the file and the attachment, and then empty the computer's deleted items file.

Use hard-to-guess passwords.

- Passwords should have at least eight characters with a mixture of uppercase and lowercase letters, as well as numbers.
- Change passwords frequently.
- Do not give out your password to anyone.

Protect computers from Internet intruders by using firewalls.

- There are two forms of firewalls: software firewalls that run on a personal computer and hardware firewalls that protect computer networks or groups of computers.
- Firewalls keep out unwanted or dangerous traffic, while allowing acceptable data to reach a computer.

Do not share access to computers with strangers.

- Check the computer operating system to see if it allows others to access the hard drive. Hard-drive access can open up a computer to infection.
- Unless you really need the ability to share files, the best bet is to do away with it.

Back-up computer data.

- Many computer users have either already experienced the pain of losing valuable computer data or will at some point in the future. Back-up data regularly and consider keeping one version off-site.

Regularly download security protection updates, known as patches.

- Patches are released by most major software companies to cover up security holes identified in their programs.
- Regularly download and install the patches, or check for automated patching features.

C&F EST. 1822

This material is provided for information purposes only and is not intended to be a representation of coverage that may exist in any particular situation under a policy issued by one of the companies within Crum & Forster. All conditions of coverage, terms, and limitations are defined and provided for in the policy. This material was developed as a general guide to safety from sources believed to be reliable and is not intended to provide legal, technical or other professional advice. These materials are not intended to replace any training or education that users may wish or need to provide to their personnel. Crum & Forster does not endorse any of the vendors listed in this publication, nor does it endorse the information, products or services that they offer or provide. Compliance with all Federal, State or local laws and regulations remain the policyholder's responsibility.