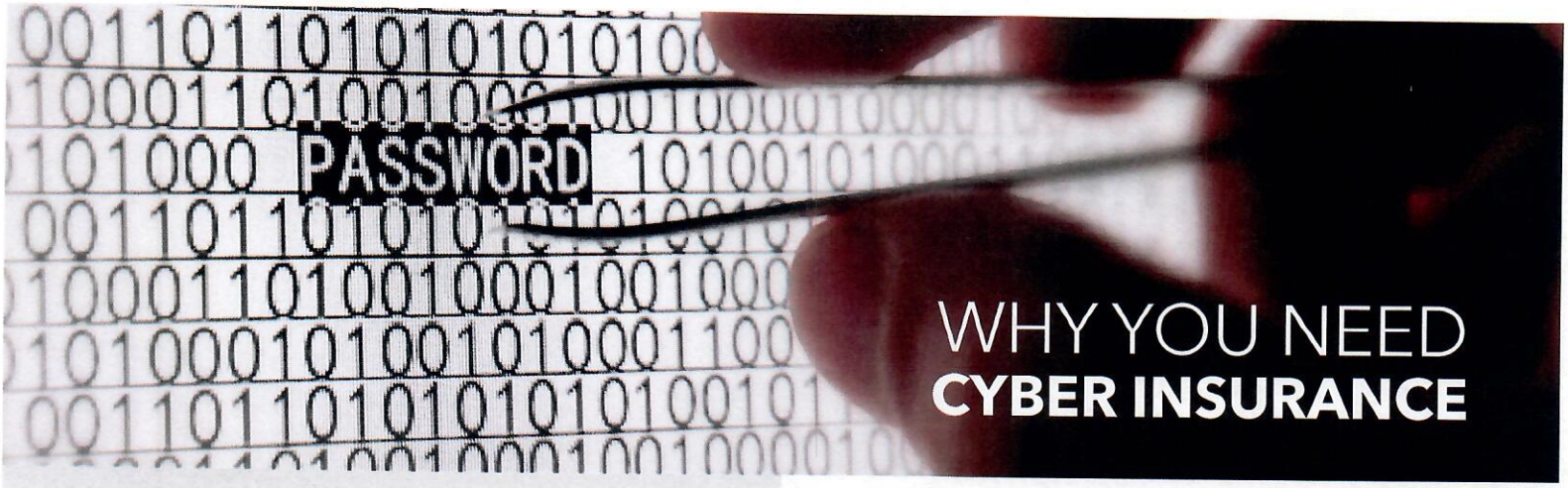

WHY YOU NEED **CYBER INSURANCE**

1 The cost of a cyber event may be significant; even for a very small business.

According to netDiligence, a leading cyber-security information service, the average cost of a cyber event for a nano-revenue sized firm exceeded $125,000.

The 2017 netDiligence claims survey also found that professional services firms are particularly exposed to wire transfer fraud. According to netDiligence, 30% of reported wire transfer fraud claims were associated with professional service firms. netDiligence found that the costs surveyed wire transfer fraud incidents ranged from $3,500 to $867,000.

2 Existing insurance is not enough.

Traditional insurance policies weren't designed for these types of risks. While your traditional insurance program might (or might not) assist you with some aspects of cyber loss event, such traditional policies will not provide coverage for significant portions of such an event. Losses not covered by traditional insurance program often include:

- Cyber incident response costs: such costs include fees to retain the services of a computer security forensic specialists to investigate an actual or suspected event, the cost to expenses to notify clients (often required by law), as well as legal costs to fully understand your firm's legal and professional obligations.
- Loss of revenues and extra expenses incurred to maintain operations after a cyber event.
- Ransomware expenses: the cost of a ransom or costs incurred to recover data without paying a ransom.
- A loss of your firm's assets resulting from social engineering fraud events. This might include:

Cyber insurance from Crum & Forster is designed to wrap around your existing insurance program in order to better protect you from these modern risks.

3 Help when you need it!

What will you do if your computers are infected with ransomware? What if a law enforcement entity contacts you indicating that they believe your computers have been compromised by foreign hackers? Do you have a plan if you are victimized by a fraudulent wire transfer scheme? Events such as these impact small accounting and law firms of every size and shape every day.

If any of these events occur, you will have 24/7 access to the Crum & Forster Cyber Response Team. Staffed with cyber-incident professionals, the Crum & Forster Cyber Response Team will assist you to formulate a plan to with an emphasis on meeting your legal and professional responsibilities. Our goal is to enable an efficient and effective response to an event that will enable you to meet all of your legal obligations and return to business as usual.

4 Meaningful assistance to prevent a loss.

We're all better off if you never have a loss. That's why Crum & Forster offers robust and meaningful loss control service. How robust? How meaningful? Crum & Forster cyber loss control services are robust and meaningful enough that we offer a significant policy discount for your participation.

Too often, "experts" make cyber security more complicated than it needs to be. Fear not! We will not be asking you to complete a long and complicated risk assessment coupled with a laundry list of loss control recommendations that you'll barely understand. We'll make it simple, effective and efficient. We'll just ask you to make a few small easy to understand changes. Changes that won't eliminate your risk, but will significantly reduce your chance of having a loss.

You should reasonably expect that participating in the Crum & Forster cyber loss control services will take less than 30 minutes during the entire policy year.

In a modern world with 21st century risks, we believe that you need modern insurance that responds to the new and evolving risks that traditional insurance products weren't designed to address. C&F Simple Cyber from Crum & Forster is designed to be comprehensive, easy to understand and provide practical solutions that enable you to concentrate on your business and your clients.

C&F EST. 1822

CRUM & FORSTER®

A FAIRFAX COMPANY

3,800 HACKING ATTEMPTS PER DAY, PER SMART HOME*

*Intersec Forum, February 2018

A COLD DARK NIGHT

Think of a cold night in February during a polar vortex. Your homeowners' in an upscale Northern Illinois neighborhood all receive an email and/or text from a stranger in some country half way around the world. It alerts them to an imminent failure in their heating and lighting systems unless they click on a link and pay a bitcoin ransom. Most of them ignore the message and find themselves in very cold, dark homes that night.

THE PAST EMPLOYEE

After an electrician terminates an employee for suspected drug use, a neighborhood suffers a mysterious flurry of home invasion thefts...all strangely without any trace of forced entry. All of the homes had security systems installed by this same employee less than a year prior. Fortunately, only the property and personal documents of the homeowners was stolen and nobody got seriously hurt.

AN EXTORTION VIDEO

Imagine feeling secure in your new smart home on your 10th wedding anniversary, celebrating in style and romance in front of a digital fireplace on your Smart TV. The next morning you get an email threatening to post a rather embarrassing movie of the runaway romantic night taken by that same Smart TV's camera...hacked since a software patch or update was delayed or missing.

Residential builders and installation contractors need more than general cyber or liability insurance. General liability policies exclude any kind of data breach. Cyber policies only pertain to data and information controlled by the builder or contractor...not the consequences of hacked Smart Home devices.

Smart Home device use (and the corresponding risks) includes, but is not limited to:

• Temperature Control • Air Quality Control • Water Quality and Pressure • Entertainment • Kitchen Appliances
• Washer/Dryer • Home Security • Garage Door Operation • Audio Controlled Lighting • Baby/Child Monitoring
• Water Heater • Coffee Maker • Smoke/CO/ Fire Detection • Sprinkler and Fire Suppression

New residential technologies can pose challenges, even nightmares for the homeowners, the builders/re-modelers and the installers involved.

The makers of the Smart Home devices don't guarantee, hold harmless and indemnify against damage/injury to your homeowner customers when their devices are hacked and fail. Catastrophic bodily injury, emotional/ mental anguish and property damage are all at risk and otherwise not likely covered by cyber or general liability. An affordable solution is needed now.

Our exclusive offering includes BOTH Smart Home device and Comprehensive Cyber coverage that can help with the many potential hacking, reputation, and technology nightmares.

WISE INSURE

www.wiseinsure.net | 866-491-9722 | exponent-marketing@wiseinsure.net

CONTRACTORS
Cyber Exposure

Contractors are not immune to losses arising from cyber attacks and malicious computer activity. According to a report from SecurityScorecard:

> *"The focus of malicious actors on the construction industry is expected to increase significantly within the coming years as construction firms begin standardizing the integration of 'smart' devices and IoT devices such as thermostats, water heaters, and power systems…These new IoT devices will create a larger attack surface that previously did not exist."* [i]

Although contractors generally handle or maintain limited amounts of personally identifiable information, they do maintain such information for employees and also often have access to third party (project related) information that may be considered sensitive by the project owners.

It is also worth noting that construction firms are increasingly relying on computers and computer systems to estimate costs, as well as to submit bids on potential contracts.

Specific concerns for construction firms include:

- **Ransomware**: Ransom expenses or the cost to repair/recreate data damages by a ransomware may be significant;
- **eCrime:** All types of firms are targets for wire transfer fraud schemes based on business email compromise or social engineering schemes; and,
- **System outage:** An extended outage of a computer system may result in significant extra business expenses or an inability to produce cost estimates or bids on job opportunities.

Key Stats

Wire Transfer Fraud & Theft of Money averaged **$179K** in breach cost .[ii]

In 2017, the average total breach cost was **$394K**, and the median total breach cost was **$56K**. [iii]

Companies with less than **$50M** in revenue were the most impacted, accounting for **47%** of cyber insurance claims. [iv]

Key Controls

- Employee training and dual-method authentication for wire transfers
- Dual authentication for remote systems access
- Timely installation of computer software updates (a.k.a. "patches")
- Regular back up of systems and data
- Restriction of administrative privileges on all work stations and computer servers.

CRUM & FORSTER®
EST 1822
A FAIRFAX COMPANY

Loss and Incident Examples

Fazio Mechanical Services : This HVAC contractor was the target of a phishing scam which introduced malware onto its systems. Ultimately, the hackers were able to gain access to the Target Corp. systems using credentials stolen from Fazio, leading to a significant breach of credit card data from Target. The impact of the Target breach was massive and included 40 million credit cards compromised and **$202 million in costs** to Target.

ASI Construction LLC[vi]**:** In January 2018, ASI was the subject of a phishing attack which targeted 2017 W-2 information belonging to employees. An individual posing as the owner emailed an ASI Construction employee requesting copies of 2017 W-2s for the workforce. The employee complied and sent the individual **336 records** containing sensitive PII.

PAR Electrical Contractors, Inc. [vii]**:** In December 2017, a thief stole a container holding daily backup tapes that, as a part of PAR's regular practices, had been taken offsite. The backup tapes were not encrypted and contained sensitive PII and PHI on employees including Social Security number,, DOB, passport number, and health information from Workers Compensation claims. Approximately **25,000 sensitive records** were exposed.

Beazer Homes [viii] **:** The company learned that from approximately September 2017 through November 2017, an unknown person remotely accessed and acquired, without authorization, emails belonging to certain Beazer employees. Approximately **118 records containing PII** were exposed.

Engleberth Construction, Inc [ix] **:** In May 2017, an employee of the company discovered that an unauthorized person, whose IP address appeared to be in South Africa, had been using her company email address. The impacted employee worked in Human Resources, and after reviewing her email activity, it was determined that she had been the victim of a "phishing" scam. Around **181 records were compromised.**

Key Coverage Considerations

- The Liability coverage part of a cyber policy should protect the insured for damage to a third-party system arising from a failure of the insured's computer security. Bad actors may gain access to a firm's systems with the explicit purpose of gaining access to systems operated by a client of the targeted firm
- Data breach event coverage should be triggered by an actual or suspected data breach event
- 24/7 access to a cyber event response team to assist the insured in evaluating and responding to an incident/event
- eCrime Coverage should be offered by the Cyber Insurer
- Coverage should extend to information in the custody of the insured or any third party for whom the insured is legally responsible

[i] https://www.constructiondive.com/news/how-construction-companies-can-improve-cybersecurity/424217/

[ii] netDiligence 2017 Cyber Claims Study

[iii] Ibid

[iv] Ibid

[v] https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[vi] https://www.doj.nh.gov/consumer/security-breaches/documents/asi-construction-20180301.pdf

[vii] https://www.doj.nh.gov/consumer/security-breaches/documents/par-electrical-20180205.pdf

[viii] https://www.idtheftcenter.org/wp-content/uploads/2018/07/DataBreachReport_2018.pdf

[ix] http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Engelbeth%20Construction,%20Inc.%20SBN%20to%20