coverlink INSURANCE

CYBER & DATA LIABILITY

A Guide on How to Manage Your Risk of a Breach

BUSINESS INSURANCE

CONTENTS

DISASTER IS JUST A FEW CLICKS AWAY... 4

YOU'RE NOT ALONE, AND WE CAN HELP 6

WE'RE ALL GUILTY OF THINKING 'IT COULD NEVER HAPPEN TO US' 9

WHAT TYPES OF CLAIMS ARE OCCURRING? 12

WHAT DOES CYBER INSURANCE PAY FOR? 17

THE COST OF PRIVACY 23

DATA BREACH CAN CAUSE SEVERE EMOTIONAL AGONY 26

10 REASONS WHY YOU NEED CYBER INSURANCE 29

RESOURCES AVAILABLE 32

Just the thought of a breach of the personal information stored for clients or employees is so overwhelming, many business owners choose to ignore the risks and consequences. You have just taken the first step to better understand the risks you face as a business owner. Hopefully you never find yourself in a situation where highly sensitive and protected information, entrusted to you in some manner, has been compromised. However, if it does happen...

ARMED WITH THE INFORMATION AND RESOURCES YOU'LL FIND IN THIS EBOOK, YOU CAN BE PREPARED TO RESPOND IN A WAY THAT MINIMIZES THE DAMAGES.

This eBook is designed to help you with the insurable disasters associated with the risks of Information Technology, sometimes referred to as Cyber Liability, Data Breach, Privacy Liability, or Network Security. Regardless of the description, the fact is, new risks require new knowledge and new practices. As a responsible business owner, you need to be aware of your exposures before you can begin to understand your options for mitigating or transferring your risk of a catastrophe.

DISASTER IS JUST A FEW CLICKS AWAY...

Do you know the most popular password on the internet? Would you believe it's Password123? While hackers certainly present a real threat to the security of our most valuable information, we as consumers need to start doing a better job of securing that information. Check out how easy it was for the Jimmy Kimmel Show to get consumers to provide their password... on television no less!

We need to do a better job of securing our sensitive information.

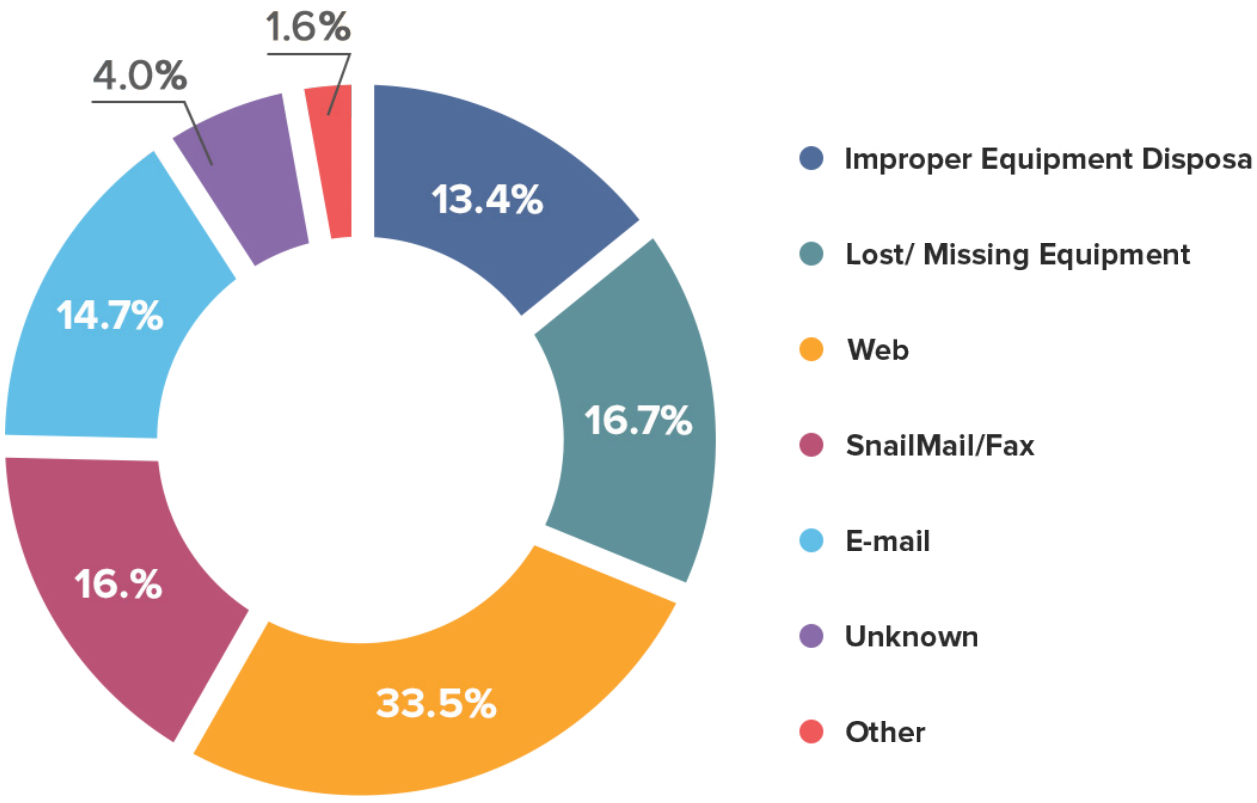
Pretty sobering stuff when you think that all the money in your personal and corporate accounts is just a password away from manipulation! But I'm sure you always create great passwords, right? And you have them committed to memory, and not stored on a sticky note or sheet of paper under your keyboard, right? Just in case, here are a few tips on creating good passwords – IT experts often say "passwords are like underwear, you should change them often" – maybe not every day, but certainly don't share them, and don't put them on a sticky note. Consider using a password manager.

Passwords don't just protect your money. All organizations and businesses are subject to hundreds of privacy laws requiring we keep information and data private. However, as breaches like Target and Sony show us, no one is immune from a hacking attack, and the consequences can be quite costly – especially for those that are unprepared.

YOU'RE NOT ALONE, AND WE CAN HELP

The good news about cyber liability is that the risks are largely understood, and often avoidable with security procedures and training. In fact, security is already incorporated into much of the technology we use every day, often without us even knowing. For example, do you have an iPhone? If yes, did you know that if you've created a password for your phone, then all messaging and emails you transmit from your phone are encrypted? Isn't technology great? Not so fast...

Inside-Accidental Incidents by Breach Type: All Time



Risk Based Security, Inc., Data Breach Intelligence.
Retrieved from http://bit.ly/1CtO6iV

Unfortunately, we can't rely on technology to solve our security problems. Why? Mostly because the problem is not technology, it's us! Did you know that most data breach cases involve acts such as opening links in emails and visiting websites infected with malware? In addition, lost, stolen or hijacked mobile devices, as well as unintended disclosure of credentials account for numerous data breach claims each year.

It's not a question of whether you will be hacked, its just a question of when...

If this seems overwhelming, not to worry, resources are everywhere for small businesses. A good place to start if you're looking for a step-by-step process to manage your cybersecurity risks is this 25 item checklist with practical recommendations for businesses.

WE'RE ALL GUILTY OF THINKING 'IT COULD NEVER HAPPEN TO US'

Prior to 2006, the world's largest media companies, our largest industrial organizations, our insurance companies, the U.S. Government, and just about everyone else who has ever been connected to the internet had already been hacked. That's not our opinion, that comes straight from FBI Special Agent Corey Collins. The bottom line is, there's no point in thinking it can't happen to us. There's no such thing as a full-proof security procedure a business can follow to guarantee their data is safe.

For a visual explanation of what's happening in our world, in real-time, check out this site that shows live DDoS attacks occurring all over the world. DDoS (Distributed Denial of Service) is a denial of service attack that attempts to render a server, or an entire network resource, unavailable to users. Talk about a sobering visual.

The reality is, hackers are after easy targets (including Target), but there are numerous resources that businesses, especially small businesses, can deploy to mitigate the risks, protect themselves, and protect their customers.

The National Cyber Security Alliance has tips to keep your business safe online, the Federal Communication Commission can help you create your own custom cyber planning guide, and the Council of Better Business Bureaus offers businesses toolkits for Data Security Made Simpler, and Data Privacy for Small Businesses.

Even if all the tools and resources at our disposal are fully utilized, unfortunately, in our world today, it's no longer a question of if you will be hacked, it's just a matter of when.

IS PRIVACY THE NEW CURRENCY?

Based on the flood of data breaches occurring every day, the regulatory implications of a breach, and the legal costs associated with responding to the breach, we could safely assume the answer to this question from an attorney's perspective is a resounding **'yes'**.

However, before you ever need to speak with an attorney about privacy laws, there is much you can do to avoid the possibility. In short, be proactive.

You likely already know that privacy laws apply to your business, so take steps to implement, document and enforce information & data procedures. Next, secure the proper and adequate insurance coverage that will respond to mistakes, attacks, fraud, and regulatory actions, fines and penalties.

It's estimated that there are several hundred Federal, State and community privacy statutes – but even attorney's won't forecast how many apply in any given information security breach.

If you're in the healthcare industry, you should know about HIPPA. If you're using credit cards, you should be compliant with PCI standards. And if you work with children, you need to be aware of FERPA. But how could you possibly know about every other statute that may apply to your business, anywhere in the U.S, or even abroad?

Transferring these types of exposures from an unknown risk by way of insurance is legal, and often times, the most cost-effective solution. Just ask an attorney.

WHAT TYPES OF CLAIMS ARE OCCURRING?

We're often asked about the types of claims or breaches affecting businesses, and while national headlines grab our attention when a major retailer like Home Depot is attacked, the truth is, there are hundreds of small businesses suffering these attacks every day. We often don't hear about them because the amount of data stolen is not substantial compared to a fortune 500 company. But to the small business that suffered the breach, it's usually severe enough that they never fully recover and often times, have to close their doors.

- **STOLEN LAPTOPS**

A regional retailer contracted with a third party service provider. A burglar stole two laptops from the service provider containing the data of over 80,000 clients of the retailer. According to applicable notification laws, the retailer – not the service provider – was required to notify the affected individuals. Total expenses incurred for notification and crisis management alone was nearly $5,000,000.

- **ROGUE EMPLOYEE**

An employee learns she may be terminated, and in response, she steals names, addresses, social security numbers and other personal information from customer files. She sold the information to her cousin who used the identities to fraudulently obtain credit cards. The affected individuals filed suit against the company for identity theft.

- **SMALL BUSINESS HACKED**

A business is hacked by a local teenager who stole social security numbers and bank account data from customer files. He sold the information to an internet website which used it to create false identities for criminals to use. The business incurred notification and credit monitoring costs, and the legal expenses as well as the damages from potential lawsuits resulted in more than $500,000 in damages.

- **MANUFACTURER DUPED**

A manufacturer located in northeast Ohio nearly transferred $315,000 to China based solely on an email request to pay for raw materials that appeared to be legitimate (full story here). If you think this couldn't happen to you, or that you would easily be capable of uncovering the fraud, you might be interested to know that the FBI released information indicating that thieves had stolen $215 million over a 14 month period using this exact scam. Certainly, those businesses that were victims thought it couldn't happen to them too.

- **SPYWARE VIRUS**

A man sent an email to his ex-girlfriend hoping to monitor what she did on her computer. She opened the email on her work computer, and over the course of two weeks, the spyware emailed the man more than 1,000 screenshots of confidential data on 150 customers. The business incurred notification and credit monitoring expenses for the affected customers.

- **DUMPSTER DIVING**

A woman looking for coupons in a large recycling bin found records containing social security numbers and medical histories. The papers came from a local medical office, and included details about more than sixty patients, including drugs they were taking, and whether they were seeing a psychiatrist. The papers were tossed by an employee with an otherwise long and stellar service record. The incident constituted a breach of HIPPA, and resulted in governmental fines against the medical office.

- **DATA THEFT EXTORTION**

A U.S. based information technology company contracted with an overseas software vendor. The vendor left certain "administrator" defaults on the company's server and a "hacker for hire" was paid $20,000 to exploit the vulnerability. The hacker demanded an extortion payment, otherwise he would post records of millions of registered users on a blog available for all to see. The extortion expenses and payments are expected to exceed $2,000,000. Do you think you would pay? If your answer is no, you might want to read up on Cyber Extortion: A Growth Industry.

DATA & INFORMATION SECURITY

The internet brings the world to our fingertips... a powerful tool capable of making our lives so much easier, creating an untold number of opportunities that would have been nearly unfathomable just twenty years ago. Unfortunately there's a downside... too many fingertips being up to no good.

Scams, bugs, viruses, spyware, crime and cyber nuisances affect everyone, and every business.

As technology works to keep pace with increasing demands for performance and security, it's inevitable there will be hiccups and the occasional disaster. There is so much we can do to mitigate this, but perhaps just being aware of the risks is the most crucial.

We've heard some techies say "you can't solve security with technology alone, you need people". We all need to be aware that security is a process, that a breach is inevitable, and to train so that we're ready when it occurs. We need to have an incident response plan, to understand that it's a continual process, and that we need to make incremental improvements to our awareness and our response.

It's a joint responsibility; a new one we're largely unprepared for because the technology is complicated and few of us are experts. But that excuse does us no good when a breach occurs, so we need to do our best to prepare... now! We need to learn security protocols, develop strong passwords, and allocate the resources necessary to properly and adequately respond when the breach does occur. Cyber insurance is just one piece of the solution.

WHAT DOES CYBER INSURANCE PAY FOR?

First, it may help you to understand where we are from an insurance industry perspective. The insurance contracts (better known as the policy) in use today are largely the exact same as they were 50 years ago. Minor changes have been made over time, exclusions added for things like mold and terrorism as these risks became more apparent, but by and large, mostly unchanged. These policies have been court tested, time and time again, and nearly all insurance companies have adopted the same language as the standard in the industry.

There is no standard Cyber Liability Policy.

Cyber is a whole new animal. There is no standard policy. Each company offering coverage has developed their own list of coverage options available and exclusions included, which is great for consumers because so many different options exist. However, it presents a challenge in that no standard cyber policy is available that consumers, Insurance Advisors and even court systems can use as a benchmark.

The importance of actually reading an insurance policy has never been more critical. It's also important to note that information provided in this eBook is current as of publication, and could become obsolete quickly. This content is not intended to be legal advice, and it should not be used as a guide to purchase a specific policy. Cyber insurance is hugely complex, and since each policy is different, only

a licensed Insurance Advisor is equipped to assist you in developing the specific policy to adequately protect your business.

Cyber insurance typically reimburses the costs you incur in the event of data or information breach. Costs vary considerably depending on the circumstances, the types of perils involved, and the extent of the damage caused.

For example, having your credit card transactions skimmed for a week is vastly different from receiving a lawsuit by a competitor for comments made by an employee family member on social media – which interestingly, has already happened!

As mentioned previously, there are no standard cyber insurance policies. Insurers offer a wide variety of options, but each is distinct. We strongly recommend reviewing your basic exposures, as outlined below, and then matching your needs to the policy best suited for your business. A Licensed Insurance Advisor can help you with this process.

FIRST PARTY COSTS:

Coverage options in this section of a policy are designed to respond to losses sustained directly by the business (the first party – you). Often times, when a business experiences a data breach, they also suffer a loss or damage to their internal systems. For example, if a virus infects your email and is distributed to your entire network, you could be looking at two distinct exposures. First, you

could be liable for the damage caused by the virus to other networks. In addition, your internal system would need to be repaired. The repair of your internal system is referred to as a first party exposure.

Examples of first party exposures include:

- **Business Interruption and Extra Expenses** – a breach occurs that causes your business a loss of income until systems are fully restored. This coverage is designed to reimburse you for your loss of income (Business Interruption) during that period of time, as well as the costs you incur (Extra Expenses) to minimize your downtime such as the costs to repair, replace or restore your data.

- **Dependent Business Interruption** – if you rely on the system of a third party to conduct your business, and you would suffer a loss of income if that system were unavailable, you might consider including this coverage in your policy. If you use a Cloud based system, check the contracts, it's unlikely they will pay for your 'loss of profits' even if they eventually restore your data and your functionality

- **Extortion** – in this situation, your personal data is the hostage. You receive a threat demanding compensation or your compromised data will be released.

- **Data Reconstruction & System Damage** – costs you incur to retrieve, restore or replace your computer programs, systems or data.

- **Reputational Harm & Public Relations** – even when a data breach causes little damage to internal systems, public knowledge of the breach can have far reaching implications detrimental to the reputation of the business.

- **Regulatory Actions & Investigations** – costs, expenses, fines and penalties resulting from a regulatory investigation.

- **Breach Notification Costs** – expenses you incur to notify customers about a breach.

- **Computer Crime** – this is the fastest growing law enforcement issue… why? According to FBI Special Agent Corey Collins, "because it's easier, safer, pays better and if caught, the penalties are significantly less." For example, walk into a bank with a gun and get away with the average heist (about $2,000) and you'll do a minimum 7 years in jail. Conversely, steal $250,000 online from the same bank and your first offense is a measly 6 months in jail.

THIRD PARTY LIABILITIES:

In these situations, the insurance company is making a payment to someone else because of the damage they suffered, which was in some way caused by you. In our previous example where your email is infected with a virus, and is distributed to your entire network, the damage caused to the systems of those who opened your email would be a third party liability.

Examples of third party coverage options include:

- **Cyber Liability** – loss arising from a hacking attack or virus that emanated from, or passed through, your computer system.
- **Privacy Liability** – breach of any personally identifiable information, including credit card information, personal healthcare information, and employee personal information.
- **Breach Notification Costs** – if you incur a breach that results in one of your clients being responsible for notifying all affected individuals.
- **Multimedia Liability & Advertising Injury** – defamation, emotional distress, intellectual property rights infringement or invasion of rights of privacy.

Christian, CIC, RPLU, Chris. Cyber Insurance Basics. 2014. Kindle

THE COST OF PRIVACY:

WHY DATA BREACH LIMITS ARE SO IMPORTANT

What does it cost if your systems are breached? According to a Ponemon Institute report, the average data breach in the U.S. costs $145 per record and the average cost per breach incident was $5.9 million. Costs vary by industry with healthcare at a whopping $359 per record and retail at $105.

Data Loss Expenses

Statistics from the Ponemon Institute 2014 Cost of Breach Study:

- Average total cost per reporting company: $5.85 million
- Average per-record cost of a data breach: $145 Globally, $201 US (Expect about $37 per record for notification and credit monitoring)

Per Capita Costs of a Breach by Industry Classification	
Healthcare	$359
Financial	$206
Hospitality	$122
Retail	$105
Communications	$177
Education	$294
Pharma	$227
Average	$145

Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis. Retrieved from http://ibm.co/1uGcqdr

If you're interested in your specific financial exposure as a result of a breach, we recommend using a Data Breach Calculator where you can take a free assessment, tailored to your operations.

Time and time again, studies show that costs can be significantly reduced when prior planning is introduced. To be effective, the planning should include a strong security policy and development of an Incident Response Plan. Organizations that invest in a Business Continuity Management team and appoint a CISO (Chief Information Security Officer) have lower breach costs outcomes.

The most effective way to reduce breach costs after discovery is an immediate and comprehensive response. Strong cyber insurance policies should include Crisis Response and hands-on claim handling.

Often times, the true cost of a data breach can never be measured. For example, how do you place a value on your reputation? You know it's important, but what's the dollar amount of its worth? Public companies that are required to disclose data breaches, also must make a provision on their balance sheet, so they have some relative idea of its financial implication. Small businesses, on the other hand, often discover the costs of a data breach are ruinous.

Looking for the easy answer? Transfer your potential cost, expenses and liabilities to an insurance company that has the resources to protect your business and defend your reputation.

DATA BREACH CAN CAUSE SEVERE EMOTIONAL AGONY

If you find yourself in the unfortunate situation of a cyber loss, it could turn out to be a minor issue, or it could be devastating. We've asked people and organizations about their experiences after a cyber breach and it's sobering to hear their stories.

After the City of Akron, Ohio had its website hacked in May, 2013, it was discovered that over 30,000 entries including names, social security numbers, addresses and phone numbers were compromised. The City's CIO and his team worked tirelessly to address the breach. It was an extremely tough period for everyone. Some felt guilty, some felt personally threatened, some were fearful for their jobs even though they'd done nothing wrong. No one was prepared for the emotional turmoil, it was like being a victim of a fire or tornado.

How you respond to a breach will likely determine whether your business survives.

When asked what was the worst thing for him, the CIO said "having to walk out and face CNN and a world of reporters, it was nothing I'd ever contemplated, let alone trained for."

The City eventually recovered, but officials and employees were left with an indelible scar – from a data breach.

EVALUATING CYBER INSURANCE POLICIES

First and most importantly, understand this: they're all different! If you currently have a cyber policy, or you're in the process of evaluating several different options, you must ensure that the coverage provided by the policy you select actually meets your needs and will respond to your claims. Just because it's called a Cyber Insurance Policy, you're provided zero assurances that it will meet your needs at the time of a breach.

Cyber insurance policies cover a variety of losses, but no two insurance companies offer the same coverage, terms, conditions and incident response plans. Not only is this complicated for insurance buyers, but even insurance advisors receive no formal education or training about cyber risks when taking their insurance license examinations.

Fortunately, there are several insurance companies that provide strong support for their products, and accomplished insurance advisors can augment their knowledge with continuing education courses. However, the cyber insurance market is still basically a teenager, and many practitioners still have much to learn.

The advisors at CoverLink are members of the Associated Risk Managers (ARM) network, a private organization providing vast educational resources, and partnerships with the industry's leading cyber insurance companies. Educated, well connected, and in a position to provide the resources necessary to help small businesses wrap their arms around this cyber and data breach exposure.

10 REASONS WHY YOU NEED CYBER INSURANCE

1. Complying with breach notification laws costs time and money – remember, laws apply where your customer is domiciled, not just where you're located.

2. Third party data is valuable and you can be held liable or fined if you lose it.

3. Data is one of your most important assets, yet it's not covered by standard property insurance policies.

4. Systems are critical to operating your day to day business, but system downtime is not covered by standard business interruption insurance.

5. Cyber crime is the fastest growing crime in the world, but most attacks are not covered by standard property or crime insurance policies. Our best techies work hard at online security, but criminals operate 24/7 and new crimes are emerging almost daily.

6. Retailers face severe penalties if they lose credit card data. You don't have to be Target to be a target. Even small retailers often face hundreds of thousands of dollars in costs and fines.

7. Your reputation is your number one asset, so why not insure it? If you want to safeguard your reputation in the event of a security breach, you'll need the help of good cyber policy to respond.

8. Social media usage is at an all-time high, and claims are on the rise.

Businesses can be held liable for the actions of their employees.

9. Portable media devices and remote access have increased the risk of a loss or theft.

10. It's not just big business being targeted by hackers, but numerous small businesses too. The media focuses on large-scale breaches, but cyber attacks are quickly becoming one of the greatest risks for small businesses.

CFC Underwriting, 10 Reasons to buy Cyber Liability Insurance.
Retrieved from http://bit.ly/1Ic2wdG

RESOURCES AVAILABLE

The Advisors at CoverLink are on the leading edge of cyber insurance and developments, and we're connected to the world's leading cyber insurance companies. While 21st century technology brings greater efficiency and new ways to process business, the potential for emerging risks is increasing exponentially. We're dedicated to helping our clients navigate these new risk dynamics, while protecting the organizations we cherish, and the communities where we live.

Ask our Insurance Advisors to help you:

- Assess your cyber risk
- Evaluate what a breach may cost your organization
- Measure the quality of your cyber security
- Implement cyber awareness and data security procedures
- Establish data security standards
- Develop employee training with continuous updates
- Implement a cyber component for your Crisis Response Plan
- Match your cyber exposures with cyber insurance coverage
- Provide cost effective options to transfer cyber risks

CONCLUSION

Regardless of the amount of time dedicated to security, or the sophistication of controls, data breaches continue to occur at an alarming rate. Hackers are increasingly targeting small businesses that may not have robust security measures in place.

Standard insurance policies in existence for decades were never designed to provide coverage for these new types of losses. Most polices provide no coverage at all, and even if coverage is provided, it's extremely limited. A standalone policy dedicated to Cyber Liability and Data Breach risk ensures there is coverage not only for legal expenses and liability, but also direct costs to address the breach.

Any business that collects or stores private information, has a website or email address, or accepts credit card payments, is at risk. The use of technology has made us more efficient, but it's also increased the challenge we have of protecting private information from accidental or malicious actions.

The bottom line is this: if you don't have Cyber Liability and Data Breach Insurance and you experience a privacy or security breach, will you know what to do?

If your answer is yes, congratulations, you're among the very few business owners

that have invested the time to truly understand your exposures, and secure the proper insurance policies to adequately respond during your time of need.

However, if your answer is no, or you're unsure about how you would respond, your next step should be to request a Cyber Insurance Proposal. Once you have completed the underwriting process, you can begin to better understand your risks of loss, how you can mitigate those risks, and if you desire, how those risks can be transferred to an insurance company.

ABOUT THE AUTHORS

Matt Simon, CIC, CPCU has been a licensed Insurance Advisor with CoverLink since 2006. Prior to joining the team at CoverLink, he worked as an Underwriter with a multi-state insurance company located in Columbus, Ohio. Matt is a Certified Insurance Counselor (CIC) and Chartered Property and Casualty Underwriter (CPCU), having successfully completed the rigorous coursework and exams to earn these designations. He's the Vice President at CoverLink, serves on the Board of Directors for the Professional Insurance Agents Association of Ohio and the Associated Risk Managers of Ohio. In 2013, Matt was awarded and recognized as the National Young Insurance Agent of the Year. He can be reached at:

Phone: (937) 592-9076
Toll Free: (877) 592-9076
msimon@coverlink.com

Terry Quested joined a Lloyds of London broker in 1974, worked in London, Latin America, Bermuda and New York City before settling in Ohio in 1990. With senior marketing and management experience for insurance companies, wholesale underwriters and intermediaries, specialty insurance service companies, reinsurance brokers and insurance agents, he is a past President of Ohio's specialty lines insurance association (OAPSLO), a past recipient of the Professional Insurance Agents of Ohio Insurance Person of the Year award and currently serves as Executive Director for Associated Risk Managers of Ohio, an organization providing educational and marketing support to its member agencies.

WHAT COVERLINK CLIENTS ARE SAYING

“ Not only are the people at CoverLink working for me, but they have also become friends over the years because they are the type of individuals you can count on and who honestly care about their people from a business and personal standpoint. I would not put my business and family in the hands of anyone other than the wonderful, professional, and dedicated staff at CoverLink Insurance. Thank you CoverLink staff for a job well done!

Mark Muirhead

“ The entire team at CoverLink has been a great source of advice when it comes to protecting my family and business with insurance and sound risk management. When I have a question I simply call or email and it gets answered promptly, it’s nice having people who truly care about me and my family’s well being. I highly recommend you call them for a second opinion for your home, auto, life and business insurance needs.

Matt Brown

coverlink INSURANCE

CoverLink Insurance is an industry leading, independent insurance agency, that has been obsessively protecting and caring for its clients since 1920.

It begins with a simple question: why? Why do we do what we do? What do we believe?

At CoverLink, we care deeply about our clients. We want to be there to pick up the pieces when tragedy strikes their lives. We exist because of our unwavering commitment to, and compassion for, our clients. To us, it's about people, not policies. People have assets to protect. People have loved ones they care for and employees who depend on them. People have dreams to pursue. We believe it's our responsibility to safeguard the people we care about.

Request a Proposal

CoverLink Insurance

coverlink.com

Bellefontaine Office
200 Dowell Ave
Bellefontaine, OH 43311

Phone: (937) 592-9076
Fax: (937) 599-2568

Urbana Office
121 Miami St
Urbana, OH 43078

Phone: (937) 306-7781
Fax: (937) 653-4457

West Jefferson Office
98 E Main St
West Jefferson, OH 43162

Phone: (614) 454-6687
Fax: (614) 879-9622