ERRORS & OMISSIONS INSURANCE:
THE COMPREHENSIVE GUIDE FOR SMALL TECHNOLOGY BUSINESSES
TABLE OF CONTENTS

Introduction 03

Chapter 1: The Risks IT Professionals Face 04
Part 1: Financial Risks for IT Professionals 05
• What Triggers an E&O Lawsuit? 05
• What Do Errors & Omissions Lawsuits Cost? 06
• How Does the Cost of Insurance Compare to the Potential Cost of a Lawsuit? 06
Part 2: Legal Risks for IT Professionals 06
• What are IT Professionals Legally Responsible For? 06
• How Can IT Professionals Protect Themselves from E and O Lawsuits? 08
Part 3: Reputational Risks for IT Professionals 08
• Reputation Protection Strategy 1: Contracts, Communication, Listening 09
• Reputation Protection Strategy 2: Business Insurance 09

Chapter 2: Managing Risk as an IT Professional 10
Overview: Big IT Risk Management Mistakes to Avoid 11
Overview: How Can IT Professionals Manage Risk Better? 12
Risk Management through Software Testing 13
A Growing Market for IT Professionals 13
Software Risk Management: Liability Issues for Software Testers 13
Software Testing for Legal Compliance 13
3 Ways to Test Software for Accessibility 13
What Accessibility Laws Do IT Professionals Need to Know? 14
Software Testing for Security 15
• Security Testing: Vital for Software Companies Handling Confidential Data 15
Software Testing for Deadlines 16
• When to Test Software 16
• How to Avoid Common Software Testing Pitfalls 17
• Why You Can Be Sued for Missing Deadlines 17

Chapter 3: Errors & Omissions Insurance for IT Professionals 22
What Is Errors and Omissions (E&O) Insurance? 23
• Why Do IT Professionals Need E & O Insurance? 24
• Why Do I Need Errors and Omissions Insurance? 24
• Should Every IT Firm Have Errors & Omissions Insurance? 25
• Questions to Ask Your Agent about Your Errors and Omissions Policy 26
What Isn’t Covered by E&O Insurance? 27
What Does Errors & Omissions Insurance Cost? 27
• Estimated Cost of an Errors and Omissions Insurance Policy for a Small Technology Consulting Company 28
• Estimated Cost of an Errors and Omissions Insurance Policy for an Independent Contractor / Web Designer 28
• Estimated Cost of an Errors and Omissions Insurance Policy for a Large Consulting Firm 28
• Get Free Errors & Omissions Insurance Quotes for Your Business 28
How to Avoid E&O Claims 29
7 Strategies for Reducing the Risk of an E&O Lawsuit 30
3 Tips for Receiving E & O Insurance Payouts Every Time 31

Conclusion 31
INTRODUCTION

Today, nearly every business relies on information technology in some capacity: from maintaining a website to communicating via email and social media to storing digital data, IT provides the backbone of commerce in a variety of industries.

Often, small IT businesses – including independent contractors and freelancers – are responsible for building, updating, and troubleshooting technology infrastructure that’s essential to their ability to function and bring in revenue. As always, with that great power comes great responsibility. A relatively small mistake by a programmer or developer can lead to hours of downtime, exposure of sensitive customer data, and lost revenue for clients. When such losses occur, clients often turn to the courts to seek compensation.

To prevent mistakes, oversights, and miscommunications from leading to costly lawsuits and lost client trust, IT professionals must embrace risk management in every project they complete. This eBook explains how IT professionals can manage the many risks they face with help from…

► Software testing.
► Client and employee education.
► Contract implementation.
► Insurance policies.

Read on for practical tips on minimizing your risks, real-life examples of what can go wrong in IT, strategies for dealing with problems, and techniques for keeping your business and your revenue safe no matter what happens.
CHAPTER 1
THE RISKS IT PROFESSIONALS FACE

PART 1: FINANCIAL RISKS FOR IT PROFESSIONALS
► What Triggers an E&O Lawsuit?
► What Do Errors & Omissions Lawsuits Cost?
► How Does the Cost of Insurance Compare to the Potential Cost of a Lawsuit?

PART 2: LEGAL RISKS FOR IT PROFESSIONALS
► What are IT Professionals Legally Responsible For?
► How Can IT Professionals Protect Themselves from E and O Lawsuits?

PART 3: REPUTATIONAL RISKS FOR IT PROFESSIONALS
► Reputation Protection Strategy 1: Contracts, Communication, Listening
► Reputation Protection Strategy 2: Business Insurance
THE RISKS IT PROFESSIONALS FACE

What types of risks threaten the strength of IT businesses? They can be divided into three categories: financial, legal, and reputational. Each type can mean disaster if you’re unprepared to handle it.

The good news? Being aware of how these risks threaten your business is the first step toward preventing disasters.

PART 1: FINANCIAL RISKS FOR IT PROFESSIONALS

For small IT firms, the biggest financial exposure (besides not bringing in enough revenue) comes from the threat of lawsuits. While you may think you’re unlikely to be sued, the reality is that more than half of all lawsuits against U.S. companies target small businesses. And small companies pay more than $35 billion per year out of pocket to defend themselves against lawsuits. As an IT professional, you need to prepare for possible lawsuits and work to prevent them so you can reduce your financial risk exposure.

Of the types of lawsuits your business might face, Errors and Omissions suits are among the most expensive. To understand how E and O lawsuits can threaten your bottom line, it’s important to know the answers to the following questions:

► What triggers an E&O lawsuit?
► What do E & O lawsuits cost?
► How does the cost of insurance compare to the potential cost of a lawsuit?

$35 BILLION = annual out-of-pocket cost of lawsuits for small businesses

What Triggers an E&O Lawsuit?

A dissatisfied client triggers an Errors & Omissions lawsuit.

When one of your clients loses money and thinks you’re to blame (because, in the client’s opinion, you did shoddy, incomplete, or negligent work, or made mistakes or oversights), they can sue you to recover their financial losses. This counts as an E and O lawsuit.

E & O LAWSUITS IN ACTION: MAJOR BRANDS VS. EPICOR

In 2012, Major Brands, a beverage distribution company, sued business software company Epicor over problems with its sales software. Major Brands claimed millions of dollars in damages after Epicor failed to install the software promptly and was unable to fix a “lag” issue that made sales entry painstakingly slow.

Assuming Epicor had an active E&O policy in place at the time of the lawsuit, it would have filed a claim on that policy with its insurance company to collect money to fund its legal defense. If Epicor had no E&O policy, it would have had to fund the lawsuit from its business assets.

Did you know?

$35 BILLION = annual out-of-pocket cost of lawsuits for small businesses
What Do Errors & Omissions Lawsuits Cost?

Lawsuits are like snowflakes – each one is unique. On the low end, a lawsuit may only cost a few thousand dollars, especially if it is dropped or dismissed by a judge. On the high end, you could pay more than a million dollars in legal fees, damages, and other expenses.

In a typical E and O lawsuit, you might have to pay for...

- Lawyers’ fees.
- Settlements to keep a lawsuit out of court.
- Witness expenses (e.g., when you hire an expert witness to testify on your behalf).
- Court fees.
- Judgments awarding damages to your client.
- Your client’s legal fees (if you lose).

Covering the cost of a lawsuit can force your business to scale back hiring or increase its prices to current customers. In fact, more than 70% of businesses dealing with a lawsuit end up doing just that. That’s not good for business.

How Does the Cost of Insurance Compare to the Potential Cost of a Lawsuit?

E&O Insurance policies typically offer coverage in $1 million increments. Your premiums will vary depending on the size of your company, the deductible you choose, and your total annual revenue.

For many small businesses, E&O premiums cost a few thousand dollars a year – much less than the six-figure legal bill you’d likely have to pay after a lawsuit. (For a closer look at the cost of Errors and Omissions Insurance, jump ahead to the section, “What Does Errors & Omissions Insurance Cost?” on p. 27.)

PART 2: LEGAL RISKS FOR IT PROFESSIONALS

We’ve established that lawsuits can cost big bucks for IT businesses. Now let’s take a closer look at the various reasons your business can be sued – in other words, at the legal risks your business faces.

In essence, your business can be sued for not upholding its legal obligations to customers, clients, or business associates. One subset of these obligations is called professional liabilities – the things you’re responsible for specifically because of your role as an IT professional.

What are IT Professionals Legally Responsible For?

Technology professionals typically have professional liabilities that fall into three categories:

- Accessibility.
- Data security.
- Copyright.

Read on for a closer look at each.
Accessibility Requirements for IT Professionals

The Americans with Disabilities Act (ADA) requires that most public physical locations in the U.S. be accessible to people with disabilities. At present, state and federal laws aren’t 100 percent clear about whether all software and web pages must be similarly accessible. In fact, the courts have gone both ways on their rulings. For a long time, judges did not assume that the Americans with Disabilities Act applied to e-commerce. But lately, the interpretation of the law appears to be shifting.

► Serving clients whose employees have disabilities. If you’re designing software for a company with disabled employees, you will probably have to accommodate their accessibility concerns. The specifics will depend on the needs of your client’s employees. If you’re designing an IT solution for a company with blind employees, for example, the American Foundation for the Blind put together this guide to making IT-infrastructure accessible.

► Working with government contracts. Section 508 of the Amendment to the Rehabilitation Act of 1973 requires that all government agencies make their web pages and information technologies accessible to people with disabilities. This law applies to all IT project managers hired by a government agency or its contractors.

► Working in industries with specific accessibility standards. Some industries have specific laws that govern accessibility requirements. For instance, publishers have to make eBooks available to disabled students who use them for a class. Before starting on a project, check with your client to see if any such laws apply to your project.

In 2012, as part of a settlement following a lawsuit by the National Association of the Deaf, Netflix agreed to start offering closed captioning for its streaming video (and pay almost $800,000 in legal fees).

As enforcement of accessibility laws evolves, it’s essential to make sure your business is in compliance so you don’t inadvertently do work that could trigger a lawsuit. Here are some specific situations where you might come under scrutiny or face an E & O claim for failing to meet accessibility standards.

Data Security Requirements for IT Businesses

IT professionals are responsible for maintaining the security of customer and client data. Sometimes, data security liabilities are called “cyber liabilities,” but for IT professionals, cyber liabilities are usually considered a subset of professional liabilities. (It’s good to know, too, that most Errors and Omissions policies sold to IT professionals include third-party cyber liability protection.)

Cost of legal fees Netflix was forced to pay in a settlement over video accessibility.

$755,000
Your data security obligations are governed by three major legal doctrines:

► **State data breach laws**, which regulate how and when you need to inform customers if their data is unlawfully accessed (by hackers and others).
► **HIPAA and HITECH laws**, which are enforced at the federal level and mandate strict regulations to protect medical records and related data.
► **The Data Protection Act**, a European law that specifies how U.S. companies are required to handle data from citizens of the European Union.

Violating any of these laws can expose your business to both lawsuits and fines. HITECH outlines fines that can exceed $1 million for medical data breaches, so make sure you’re in compliance.

**Copyright Concerns for IT Professionals**

Copyright laws are of special concern for web developers and programmers, who can be sued for copyright infringement over images, videos, other media, and even the code they use.

That’s right. You could be sued for using someone else’s code. What’s more, judges have ruled that web developers who use a competitor’s brand name or trademark in their metadata (in order to rank higher in search ratings) can also be sued for infringement.

**How Can IT Professionals Protect Themselves from E and O Lawsuits?**

To recap: IT businesses are exposed to a variety of risks linked to their professional responsibilities. If they fail to uphold any of these responsibilities (or if a client believes they have failed to uphold one of these responsibilities), they can be sued.

Protecting yourself from lawsuits requires a robust risk management plan. We’ll go over what a solid risk management plan looks like for IT freelancers, independent contractors, and business owners later in the eBook (jump ahead to “Managing Risk as an IT on p. 10 to take a look at that now). In essence, though, effective risk management includes contracts, communication, client education, and adequate business insurance.

**PART 3: REPUTATIONAL RISKS FOR IT PROFESSIONALS**

Given the financial and legal exposures IT companies face, you might be surprised to learn that, in a recent study conducted by insurance company ACE European Group, more than four-fifths of businesses interviewed (81 percent) cited reputational risks as their most difficult to manage. Translation: the majority of companies see threats to their reputation as tougher to handle than threats to their income, property, or information security.

That’s pretty significant. What’s even more telling, though, is the reasons the surveyed companies gave for counting their reputational risk among their hardest to handle:

► **77 percent** said they had trouble assessing the financial value of their reputation. In other words, they don’t know what their good name is worth and so don’t know how much to invest in protecting it.
► **68 percent** said they didn’t know where to turn for reliable guidance about managing their reputational risks.
► **66 percent** admitted to feeling overexposed to reputational risk from an insurance perspective.
► **56 percent** said they feared (but didn’t fully understand) the threats to their reputation that social networks and other forms of social media presented.

So how can IT professionals protect their most valuable asset? There are two major ways.
Reputation Protection Strategy 1: Contracts, Communication, Listening

Reputation management starts with communication. The more clearly you communicate with clients, business partners, and others, the less likely you are to be the target of a lawsuit or another event that can tarnish your hard-won reputation. For an IT business, communication typically means…

► Using thorough contracts. Setting clear guidelines at the start of a project can help prevent disappointment (and E&O lawsuits alleging negligence) down the road.

► Checking in often with clients. Communicating any plan changes, project challenges, or other important points as they happen can prevent unpleasant customer surprises (and lawsuits).

► Monitoring the conversation online. Social media search functions and alerts make it easy to keep track of what people are saying about your business online. Keep an eye on unhappy (or really happy) customers, listen to what they’re saying, and engage with them when possible. Many potential blowups can be prevented by demonstrating that you care about your customers and are genuinely willing to help them.

Reputation Protection Strategy 2: Business Insurance

The ACE study’s finding that business owners are super-focused on protecting their reputation highlights a reality of the Internet age: in an information- and advertising-saturated world, it’s often the opinions of our friends and family that carry the most weight. These opinions (and the way they’re expressed on social networks and through word-of-mouth communication) can significantly influence a person’s decision to work with a given company, whether or not those opinions are supported by facts.

In other words: what your potential customers think about your business is vitally important to your ability to win them over.

Imagine, then, that you’re hit with a lawsuit claiming that you lifted code from an existing application or piece of software. Or that one of your clients is victimized by a massive data breach and claims it was your business’s shoddy network installation that allowed the breach to happen.

Even if you aren’t actually at fault in either situation, chatter on social media sites or coverage on news outlets is enough to seriously batter your reputation, forever linking your business to subpar service in your potential clients’ minds.

E and O Insurance helps you manage that risk by giving you the financial muscle necessary to nip negativity in the bud and take control of the conversation about your business. In the third part of this eBook, we’ll delve into how E&O Insurance works in more detail.

81% OF COMPANIES say their reputational risks are the hardest to manage.
CHAPTER 2
MANAGING RISK AS AN IT PROFESSIONAL

OVERVIEW: BIG IT RISK MANAGEMENT MISTAKES TO AVOID

OVERVIEW: HOW CAN IT PROFESSIONALS MANAGE RISK BETTER?

Risk Management through Software Testing

A GROWING MARKET FOR IT PROFESSIONALS

SOFTWARE RISK MANAGEMENT: LIABILITY ISSUES FOR SOFTWARE TESTERS

SOFTWARE TESTING FOR LEGAL COMPLIANCE

3 WAYS TO TEST SOFTWARE FOR ACCESSIBILITY

WHAT ACCESSIBILITY LAWS DO IT PROFESSIONALS NEED TO KNOW?

SOFTWARE TESTING FOR SECURITY

► Security Testing: Vital for Software Companies Handling Confidential Data

SOFTWARE TESTING FOR DEADLINES

► When to Test Software
► How to Avoid Common Software Testing Pitfalls
► Why You Can Be Sued for Missing Deadlines

SOFTWARE TESTING FOR VALIDATION AND VERIFICATION RUSH JOBS: DEALING WITH CLIENT EXPECTATIONS

Risk Management through Client Education

WHY CLIENT EDUCATION IS YOUR MOST POWERFUL ANTI-DATA-BREACH TOOL

WHAT IS FIRST-PARTY LIABILITY?

WHAT IS THIRD-PARTY LIABILITY?

Risk Management through Contracts

CONTRACT BASICS FOR IT PROFESSIONALS

PROTECTING YOUR BUSINESS WITH CONTRACTS

ESSENTIAL CONTRACTS FOR IT FIRMS: NDA, PRIVACY POLICY, & WEBSITE TERMS OF USE
MANAGING RISK AS AN IT PROFESSIONAL

Now that you know where your business is vulnerable, you’re probably eager for strategies to reduce your risks. That’s good: a comprehensive risk management plan is an IT professional’s best friend. This section explains how to implement three key layers of a solid risk management plan:

► Testing
► Client Education
► Contracts

The fourth essential piece of the risk management puzzle, Errors and Omissions Insurance, is a big topic. We decided to give it its own section. Read on to get an idea of what you can do internally and externally to prevent the kind of incidents that lead to expensive liability suits. If you’re curious about what might happen when, despite your best efforts, you’re faced with a liability suit, jump ahead to the section on E&O Insurance (it starts on p. 23), where we go into all the juicy details.

But before we plunge into the specifics of risk management for technology freelancers, independent contractors, and small-business owners, let’s review the basic principles of risk management.

OVERVIEW: BIG IT RISK MANAGEMENT MISTAKES TO AVOID

Performing IT risk assessment and risk management is a crucial part of maintaining security day to day. Even if you’re not conducting formal risk analysis on a daily basis, chances are you’re doing the little things that strengthen your overall risk management strategy: updating passwords, updating software, logging out of machines when you walk away, and keeping your office locked.

But are you leaving yourself and your clients exposed to data breaches, hackers, or viruses through channels you’ve overlooked? If so, you could be making one of these three common risk management mistakes, which cost too many IT businesses time, energy, money, and reputation:

► Forgetting about the risks your clients present.
  Whether you provide advice as an IT consultant, offer leadership as a project manager, or design and build site infrastructure, your clients expose you to serious cyber risks every day. Why? Because of something called third-party liability. The cyber risk that tends to be at the top of people’s mind is called first-party: the risk that your databases could be exposed by hackers. But if you set up an operating system for a client and that OS later permits a breach, you could be held liable for your role in causing it.
Underestimating the impact of human error.
Sure, you’re careful about maintaining your passwords and locking your tablet after you’re done, but are your employees? Are your clients? A Verizon data breach study conducted in 2013 found that 74 percent of data breaches are “opportunistic” attacks, meaning that they happen because hackers notice a vulnerability that they decide to exploit. Translation: we can prevent about three-quarters of data breaches by better protecting our data. Keep in mind that the less tech-savvy your clients are, the less likely they are to recognize the importance of protecting their data and equipment.

Overlooking big-picture risk exposures.
It’s easy to get bogged down by focusing on the individual risks that threaten your company and forgetting to take a step back to look at the bigger picture. But often, you can save yourself time and money by making a single big change (e.g., purchasing antivirus software for all your employees who use mobile devices for work purposes, rather than addressing individual virus incidents as they arise). Of course, knowing which changes to make requires you to step back from time to time and analyze the larger context of various security events.

OVERVIEW: HOW CAN IT PROFESSIONALS MANAGE RISK BETTER?
The good news is that, regardless of where your major risks are, the same basic rules of risk management apply. Those rules include...

- Establish and enforce data security protocol. Update passwords regularly, update software as patches emerge, buy antivirus software, and limit access to sensitive data.
- Educate your clients about their role in keeping their data secure and preventing breach incidents. Encourage clients to purchase first-party Cyber Liability Insurance to cover the costs of any data breaches that happen.
- Communicate new risks with clients as you become aware of them. As the IT guru, you’re more likely to have a handle on the latest viruses and security patches that might affect your clients. Do them the favor of alerting them to new threats, and you’ll make yourself more valuable while minimizing your exposure to third-party cyber liability.

Read on for a more detailed look at how you can manage your risks through software testing, client education, and the use of strong contracts.
Risk Management through Software Testing

A GROWING MARKET FOR IT PROFESSIONALS

The outsourced software testing market is expected to grow more than ten percent by 2016, according to a study done by Technavio, a leading technology research firm. While this growth presents an opportunity for IT professionals to expand their business, it also means small-business owners in IT fields need to be aware of the risks of this emerging industry.

SOFTWARE RISK MANAGEMENT: LIABILITY ISSUES FOR SOFTWARE TESTERS

Can software testers be sued for failing to identify bugs and security weaknesses in client software? Yes. This is a major area of professional liability for software testers. Software testers can be sued for professional negligence when they don't test software thoroughly, overlook an error in their testing, or otherwise fail to deliver the quality of work expected from clients and outlined in contracts.

As you know, it can be nearly impossible to find every defect or security hole in a piece of software. Software giants like Microsoft frequently update their programs after they become aware of new security threats (read about one update to Word and Windows Microsoft made after it learned of the new vulnerability.). While you can't expect to find every flaw, you can practice smart software risk management by protecting your company with IT business insurance.

As you prepare to meet the growing demand for software testing, remember that liability goes hand in hand with opportunity.

SOFTWARE TESTING FOR LEGAL COMPLIANCE

We mentioned earlier that ensuring accessibility of software may be a legal responsibility for IT professionals. Here's a closer look at strategies for testing software to ensure that it complies with applicable accessibility standards.

3 Ways to Test Software for Accessibility Requirements

In its web accessibility handbook, Microsoft suggests that software testing should consist of three phases:

1. **Functional testing.** Do all the features of the website, service, or software work? This is the most basic component of testing: finding potential software defects.

2. **Usability testing.** Is the service or software easy to use for people with and without disabilities? Many usability concerns are universal. For instance, having a clean, easy-to-read interface helps all users.

3. **Compliance testing.** Are there compliance standards you need to meet? Depending on your situation, you may have to meet protocol outlined by the Americans with Disabilities Act of 1990, Individuals with Disabilities Education Act (IDEA) of 1997, the Assistive Technology Act of 1998, W3C web accessibility standards, or other guidelines. We’ll outline these requirements below.

**OF NOTE:** You don’t have to be the author of software code to be held liable for errors. If you played a role in testing the software and didn’t catch a problem, you could be held liable for damages the problem caused (i.e., be held responsible for financially compensating affected parties).
Testing software for accessibility can involve all sorts of things. For instance, to make software accessible for the visually impaired, software testers check how well a screen-reader program is able to process information and how accessible the navigation is via keyboard alone.

Some businesses (including the SSB BART Group) specialize in testing software for accessibility and offer accessibility training for IT professionals who want to learn more about designing software and systems to be handicap-accessible. Its website also posts a thorough overview of accessibility testing procedures.

**What Accessibility Laws Do IT Professionals Need to Know?**

There may be specific laws that you need to know that are unique to the clients or industries you serve, but the following list outlines the accessibility laws that most commonly affect IT businesses.

- **Americans with Disabilities Act.** Section 504 requires that public programs be accessible to people with disabilities. Any work you do for federal government agencies, local governments, educational facilities, or other organizations that receive government funding will need to be handicap-accessible. Employers must make software and IT systems accessible to all employees.

- **Individuals with Disabilities Education Act (IDEA) of 1997.** This law requires states to make public education accessible to students. Education software or IT systems you install at schools or libraries will have to meet accessibility standards.

- **The Assistive Technology Act of 1998.** This law provides money to state programs to make accessible devices, software, and technology available to disabled citizens. You might work on one of these projects as a contractor or subcontractor.

- **Telecommunications Act.** Section 255 requires that any telecommunications (VOIP, computer-automated answering systems, etc.) be accessible or compatible with assistive technology to make them accessible. The FCC published a guide to accessible telecommunications.

- **W3C web accessibility standards.** While not a formal law, these international guidelines are industry-standard ways to make websites and designs accessible to all users. The W3C even has a series of validation programs that can test your software for errors, including one called HTML TIDY, which cleans up HTML coding errors and finds places where you can make your site more accessible to the disabled.

Whether you’re a programmer, web designer, or software consultant, the general takeaway is that failing to test software for accessibility can expose your business to professional liability lawsuits.

**EXPECTED GROWTH** in outsourced software testing market by 2016

10%
SOFTWARE TESTING FOR SECURITY

Any software or web app can have security vulnerabilities – just ask Google, which recently announced that it fixed a bug that allowed hackers to steal passwords from Google accounts.

CASE IN POINT: A Google Bug

In 2013, a security expert discovered a Google bug that allowed him to exploit a weakness in the way Google Web Apps work. The security expert sent a link via email that announced a user’s password was stolen and requested they reset their account information.

When users clicked on the link, they were taken to Google’s account reset page. What users didn’t see was that after they clicked, they were momentarily taken to the attacker’s page, which ran a script that would steal their new password and authentication data after they entered it. A flaw in Google web apps allowed this mirroring. Unfortunately, if you keep track of cyber security news, you’ll read stories like this every week.

The prevalence of security attacks – even at the world’s best-known companies – emphasizes how important it is for your business to test software for bugs and security weaknesses so you can avoid the reputational damage and high costs associated with data breaches.

Security Testing: Vital for Software Companies Handling Confidential Data

In addition to triggering fines for enabling or failing to prevent data breaches, security bugs in software or web services can lead to cyber liability lawsuits when they cause data leaks. As cyber threats grow, testing software becomes increasingly crucial.

To adequately manage the risks posed by cyber criminals, a software testers’ risk management plan should do the following…

► Maintain high levels of security. Twitter recently announced that it was enabling forward secrecy encryption for user data. The social media company is following the recent trend of other web giants (Google, Dropbox, and Facebook), which are taking extra steps to guard user data. Perfect forward security encrypts each session between users and company servers with a unique encryption key. Because each session is uniquely encrypted, it limits the amount of data hackers can steal and makes data harder to decrypt. As the owner of an IT business, it’s your legal responsibility to stay on top of trends in cyber security, updating security protocols to reflect new developments and prevent new, more sophisticated attacks. Whether that means encrypting data, educating employees, or installing high-quality security software on your computers, you need to act as a steward for user data, guarding it from hackers and data breaches.
► **Test for security.** The Google example mentioned earlier emphasizes how important software testing can be. Software testing can reveal a potentially devastating vulnerability before it’s too late and prevent you from being sued. But it’s important to keep in mind that even after you deliver software to clients, you are responsible for making sure it isn’t vulnerable to attacks. What does that mean for small IT companies? You may have to update software in response to new malware and other threats.

► **Protect your business from the fallout from client data breaches.** If, despite your best efforts, one of your clients suffers a data breach that can be linked to software you tested, that client might sue you to recover some of the losses linked to the breach. How much might that be? The Ponemon Institute, a cyber security research group sponsored by Symantec, found that [cyber breaches cost $188 per stolen record](http://www.ponemon.org) in 2012. If your client’s breach was small – say, 100 records – that would mean a $18,880 bill, which is well beyond what most software testers can easily afford. Luckily, most Errors & Omissions Insurance policies sold to IT professionals include coverage for lawsuits over client data breaches. This type of protection is called third-party Cyber Liability Insurance.

### SOFTWARE TESTING FOR DEADLINES

Sticking to deadlines and meeting software-testing milestones are important for software developers and other IT professionals who want to limit their liability and prevent lawsuits. Why? Because missing deadlines established in a contract can lead to breach-of-contract lawsuits. IT professionals can avoid these suits by knowing…

► When to test software.
► How to avoid common pitfalls in the software testing process.
► Why they can be sued for missing deadlines.

**When to Test Software**

You know the saying: The early bird catches the worm. In this case, the early bird catches the bug. The earlier you test, the better able you are to incorporate feedback from tests and catch errors before they become more problematic. This applies to both functionality and usability testing.

Microsoft, in its article “[Testing in the Software Lifecycle](http://www.microsoft.com/en-us/download/choose-what-to-download-53.aspx),” advocates for testing early and often, noting that “the software development lifecycle is one in which you hear of a need, you write some code to fulfill it, and then you check to see whether you have pleased… users, owners, and other people who have an interest in what the software does.”
Though it seems like more work, Microsoft argues that an incremental, step-by-step testing process is a vital way to reduce costs and waste and, ultimately, ensure happy clients.

Google agrees, advocating for integrating testing with development. Former Google engineering director James Whitaker says programmers should “build a little and then test it. Build some more and test some more.” (Read more in his guide to how Google tests software.)

How to Avoid Common Software Testing Pitfalls

In a TechTarget interview, Doug Hoffman, a software-testing expert, outlines some of the common problems with software testing. He reminds developers that software testing is often inconclusive. He points out four common pitfalls, which testers can avoid by being aware of:

► Overlooking errors. Many software errors won’t show up in a test. If a test is designed to test the functionality of a specific feature, remember it only tests whether or not a function works. There may be other errors you can’t see. Doug Hoffman reminds developers of a number of commonly overlooked errors that don’t show up in tests, including “memory leaks, data corruption unrelated to the expected results, [and] changing of environmental variables.”

► Testing with the wrong tools. A test itself can have errors, which can lead to inaccurate results. You may be led to think everything is working correctly (or that nothing is), when in reality the problem is just in your testing software.

► Assuming functionality. Hoffman points out that a successful test only means the program functioned correctly once. Under different conditions, it may fail.

► Assuming malfunctions. Similarly, software testers may be too quick to assume there is a problem in their code. Testing conditions (or the test itself) may be causing parts of the software to malfunction.

Why You Can Be Sued for Missing Deadlines

Missing deadlines can be considered a “breach of contract” or a “misrepresentation” of the services you agreed to provide clients. Of course, many projects don’t go as planned. There are always bumps in the road. Because of the potential for lawsuits, it’s vital for you to build room in your schedule and cost estimates to accommodate mishaps and unexpected roadblocks.

Here’s an example from real life: In January 2013, Avanade (a Microsoft and Accenture joint venture) was sued for underestimating the cost of a project and failing to deliver it on time. At stake in the suit is millions of dollars in damages.

IN SUMMARY: continually integrating software testing helps IT freelancers, independent contractors, and small businesses catch bugs and errors earlier so they can deliver projects on time and avoid lawsuits.
SOFTWARE TESTING FOR VALIDATION AND VERIFICATION

People sometimes use the words verification and validation interchangeably (and often abbreviate them to V&V). While both techniques can help you avoid Errors and Omissions lawsuits, there are key differences between them.

Here's a basic explanation:

► **Validation** is the process of making sure software satisfies a client's requirements. This can include testing for and reviewing the specifications in your contract. Validation makes sure you deliver the exact product your client asks for.

► **Verification**, on the other hand, is how you test that your program works well and doesn’t have any major defects. Verification can include walkthroughs, quality control, and other usability testing.

**CASE IN POINT: HEALTHCARE.GOV’S V&V PROBLEMS**

The New York Times published a history of the troubled HealthCare.gov launch. The article notes that the website’s problems were primarily caused by two things: insufficient testing and coordination difficulties between contractors and vendors.

In part because of rushed deadlines and poor communication, IT contractors made validation errors and failed to deliver the product specified in their contract. For example, the website was supposed to be able to handle 50,000 users, but crashed with as few as 500.

By failing to build a website that met the client specifications, the programmers failed to fulfill their validation requirements.

The rush to finish the website led to insufficient software testing, which meant there were also a number of usability and verification issues. For instance, sloppy code and other problems made the website much slower than it should have been. During the initial rollout, some pages took more than eight seconds to load; now, after fixing the code, they take less than a second.

HealthCare.gov’s problems illustrate how intricately validation and verification testing are connected. If software doesn’t deliver a client’s requirements (i.e., fails validation and doesn’t function properly), you can’t perform sufficient verification tests to improve usability.

**Rush Jobs: Dealing with Client Expectations**

Most IT professionals face demands for speedy work at least once in their career. Your client wants the task completed within an unreasonable timeframe; if you agree to their deadline, you’ll have to cut corners somewhere. You’re in a difficult situation: you don’t want to tell your client you can’t meet their demands (which looks bad for your business), but at the same time you can’t risk delivering subpar work.

Remember that IT is a service industry in addition to being a technical one. You need to maintain strong client relationships, and the best way to do this is by being honest, managing expectations, and delivering a fully functioning product – not one you’ll have to debug later.
Risk Management through Client Education

Why Client Education Is Your Most Powerful Anti-Data-Breach Tool

An IT consultant’s work includes more than just installing software and setting up hardware. You may not realize it, but you are also responsible for teaching clients about cyber security. Why? Consider the example of a recent data breach at the University of Washington’s medical school.

A UW employee opened an attachment in a phishing email. The malicious software contained in the attachment led to a data breach of over 90,000 records containing Social Security numbers and payment information. In response, the medical school had to hire a cyber security crisis management firm to review its network security and notify every patient who was affected – all because of one opened email.

This news story highlights three important points about data breaches:

► Data breaches can be caused by simple, preventable mistakes.
► You can’t assume your clients understand the basics of data breach prevention.
► After one of your clients suffers a data breach, you could be named in a lawsuit as a responsible party.

To prevent the kinds of mistakes that lead to costly data breaches, IT professionals need to be aware of two kinds of cyber liability: first-party and third-party. Here’s a look at how each works and how each can affect your business.

What Is First-Party Liability?

First-party liability is what you’re responsible for in your own business. In the context of data breaches, you have first-party liability when a data breach targets your data, exposing the records of your clients or customers. Most small IT businesses have so few clients that they don’t have much first-party exposure.

Your clients, however, most likely have greater first-party liability exposures. To manage those exposures, they can purchase first-party Cyber Liability Insurance. Benefits from this type of coverage typically pay for the costs associated with a breach to their customer data, including…

► Notifying clients that their information was compromised or exposed.
► Purchasing credit monitoring services for customers affected by the breach or hacking incident.
► Launching a public relations campaign to restore the reputation of the company affected by the breach.
► Compensating the business for income it isn’t able to earn while it deals with the fallout of the data breach.
► Paying a cyber extortionist who holds data hostage or threatens an attack.

If your clients don’t have Cyber Liability coverage, however, they won’t receive compensation from an insurance provider after a data breach. Instead, they’ll have to cover the associated costs out of their own assets. To make up for having to pay all that money, they may sue any parties they think are responsible for causing or failing to prevent the breach – and if you provided IT services for them, that list could include your business.
What Is Third-Party Liability?

Third-party liability is the responsibility you have for your clients’ data. If one of your clients suffers a data breach, doesn’t have insurance, and wants to recover some of their losses, they can sue you – and depending on the circumstances, you might be found partially liable for the breach.

Here’s the kicker, though: even if you’re not found liable for causing a data breach, you may still be responsible for paying legal expenses (including lawyers’ bills) if and when a customer sues you.

The good news? You can insure yourself against the costs associated with third-party cyber liability. In fact, you may already have insurance protection for these risks. Most Errors and Omissions Insurance policies for IT firms include basic third-party Cyber Liability coverage. So if you already have an E and O policy, you likely have protection for any third-party liability your work exposes you to.

So what kinds of events might cause you to be liable for a client’s data breach?

The following are examples:

► Failure to anticipate or prevent the transmission of a virus to a third party.
  (E.g., a security gap in your software lets a virus onto your client’s machine and it spreads to all your client’s email contacts.)
► The misuse, disclosure, or theft of confidential information stored on a network.
  This is your classic data breach: one or more of the systems you set up allows a hacker to access and/or expose a client’s customers’ information.
► Infringement of the right to privacy.
  This could involve an event in which a system you built fails to keep confidential information (e.g., medical records) properly secure.

HOW TO EDUCATE YOUR CLIENTS TO REDUCE YOUR RISK EXPOSURES

These client-education strategies can help you prevent data breaches and the lawsuits they trigger.

MAKE SURE YOUR CLIENTS…

► Create strong passwords and update them regularly.
► Invest in antivirus software for all computers and mobile devices.
► Update software and operating systems with the latest security patches.
► Limit access to sensitive data (i.e., don’t give everyone access to everything).
► Log out of machines when not using them.
► Invest in first-party Cyber Liability Insurance to manage the costs of any data breaches that happen.

MAKE SURE YOU…

► Create a glossary or definitions page. If you’ve noticed that a lot of your clients have questions about certain phrases or concepts you frequently encounter in your work, create a brief glossary document you can hand out to new clients. This will help clarify key concepts from the beginning and prevent the kind of misunderstandings that can lead to lawsuits.
► Ask questions at the beginning of a contract. Before beginning a project, be sure you’re clear about what your client expects from you and about what you can reasonably deliver. Particularly when you’re working with someone who’s not especially tech-savvy, it’s difficult to over-communicate the expected parameters of a project.
► Talk through expected outcomes in detail. Many non-technical clients understand outcomes better than the components or processes that yield those outcomes. Be sure to take the time to get on the same page about what the final product will look like to prevent misunderstandings after hours of work.
Risk Management through Contracts

Structuring client relationships with contracts is essential to setting clear expectations and limiting your liability. We covered contracts in great detail in an eBook we published several years ago, but we thought the topic was worth updating. Visit the links below for highlights from the earlier eBook and read on for additional useful information on using contracts to reduce your risk exposure.

CONTRACT BASICS FOR IT PROFESSIONALS
► Contracts to Start Client Relationships Right
► Contracts You Need When Hiring a Contractor
► Client Contracts: Is There Such a Thing as Too Much Insurance?
► ASP Contracts: Keep Control, Cut Risks
► Software Licensing Agreements: Protect the Value of Your Work
► Clear Documentation = Better Results
► Employment Contract = Valuable Part of Hiring
► What Makes a Good Network Services Agreement

ESSENTIAL CONTRACTS FOR IT FIRMS: NDA, PRIVACY POLICY, & WEBSITE TERMS OF USE

As any owner of an IT business can attest, the legalities of running a business can get complicated. Between contracts, licenses, terms of use documents, privacy policies, contractor agreements, and more, there are dozens of legal forms that dictate how your business runs and what your legal responsibilities are.

Creating all those contracts can get expensive: in order to be legally binding, a contract has to meet stringent criteria, which means you’ll likely have to hire a lawyer to help. But many lawyers aren’t familiar with the ins and outs of your tech business, which means you’ll have to pay for the hours it takes your counsel to learn how your business works so that he or she can construct documents that accurately reflect the work you do and the risks you face.

Those expenses can add up quickly, making even basic contracts and legal agreements a financial strain for smaller IT businesses. But forgoing such contracts opens you up to the risk of even greater financial loss: without a limitation of liability clause in a website privacy policy, for example, you could be on the hook for tens of thousands of dollars in settlement costs if someone sues you.

PROTECTING YOUR BUSINESS WITH CONTRACTS

Through conversations with owners of small tech firms, we've found that the following three contracts are among the most in-demand. The good news? You can download free samples of each of these contracts by visiting TechInsurance's free sample contracts page.

► Mutual Non-Disclosure Agreement (NDA): This form is essential if and when you work with a business partner or contractor who needs access to proprietary information or other sensitive data (including trade secrets). It requires parties to the contract to maintain confidentiality and outlines legal remedies if any party breaches the terms of the agreement.

► Website Terms of Use (Terms and Conditions) Agreement: This contract limits the liability of a website creator. When you build a website for a client, the Terms and Conditions Agreement states that you cannot be held liable for losses that website users incur related to the content of the site. It also asserts that you do not vouch for the completeness or accuracy of information included on the site.

► Website Privacy Policy: An important contract for anyone building a website for a client, the Privacy Policy outlines how the site administrators plan to use visitors’ data and limits the website maker’s liability for losses related to data use.
CHAPTER 3
ERRORS & OMISSIONS INSURANCE FOR IT PROFESSIONALS

WHAT IS ERRORS AND OMISSIONS (E&O) INSURANCE?
► Why Do IT Professionals Need E & O Insurance?
► Why Do I Need Errors and Omissions Insurance?
► Should Every IT Firm Have Errors & Omissions Insurance?
► Questions to Ask Your Agent about Your Errors and Omissions Policy

WHAT ISN’T COVERED BY E&O INSURANCE?

WHAT DOES ERRORS & OMISSIONS INSURANCE COST?
► Estimated Cost of an Errors and Omissions Insurance Policy for a Small Technology Consulting Company
► Estimated Cost of an Errors and Omissions Insurance Policy for an Independent Contractor / Web Designer
► Estimated Cost of an Errors and Omissions Insurance Policy for a Large Consulting Firm
► Get Free Errors & Omissions Insurance Quotes for Your Business

HOW TO AVOID E&O CLAIMS
► 7 Strategies for Reducing the Risk of an E&O Lawsuit
► 3 Tips for Receiving E & O Insurance Payouts Every Time
The first two sections of this eBook dealt with managing the risks your business faces so that you can avoid Errors and Omissions lawsuits, which can be expensive, time-consuming, and disastrous for your reputation. But no matter how well you manage your risks, the reality is that you’ll still have some exposure to E&O lawsuits. This section provides information and resources you can use if, despite your best efforts, you find yourself facing an E and O lawsuit.

Read on for tips on keeping your business up and running and your revenue strong even when an unhappy client sues you over work you did.

WHAT IS ERRORS AND OMISSIONS (E&O) INSURANCE?

Errors and Omissions Insurance (also called Professional Liability Insurance) is a type of coverage that lets you operate your business without worrying that an unexpected lawsuit will force you to drain your business or personal assets. E & O benefits come to the rescue when a client claims that work you’re responsible for (such as programming, software installation, networking, etc.) includes mistakes or oversights that caused them a direct financial loss.

Those benefits take the form of payments to reimburse you for certain expenses associated with defending yourself in a lawsuit, including...

► **Lawyers' fees.** Even if an Errors and Omissions claim against you is without merit, being faced with a claim means you’ll have to present a legal defense. To do that, you’ll want to have a lawyer on your side, particularly if your case involves uncharted legal ground. E&O Insurance covers the cost of lawyers’ fees up to the limits of your policy, so that you can focus on serving your clients rather than scraping up enough money to pay your legal bills.

► **Other court costs.** In addition to paying your lawyer, defending yourself might involve paying docket fees, expert witness fees, transcript fees, and more. Luckily, these are all covered by insurance.

► **Settlements or judgments.** If you agree to settle with your client or go to court and are found liable for wrongdoing, your E and O policy will cover the settlement or judgment costs, up to the limits of your policy.

WHAT E & O INSURANCE POLICY LIMITS DO I NEED?

The kind of work you do and the type of clients you serve are two major factors that affect how high your Errors and Omissions policy limit should be. If you work with larger companies, it’s usually a good idea to have a higher E&O limit. Why? Because a mistake that prevents a large company from operating (even for a day) could cause a much greater financial loss than one that prevents a sole proprietor from operating, and you’ll want a policy that can cover these losses.
Why Do IT Professionals Need E&O Insurance?

Let's get one thing straight off the bat: not every small business needs Errors and Omissions Insurance. In some industries, there's just not a great enough risk of lawsuits to justify the cost of an E & O policy.

But if you own a technology company, you should be aware that your risk of an E&O lawsuit could well be higher than that of business owners in other industries. Here's why.

► Many of your clients don’t fully understand what you do. Because of this, your expectations for a project and theirs may not line up. When you deliver work that you think is perfect, they might be disappointed – and decide to sue. If and when such a lawsuit arises, your Errors and Omissions coverage takes effect.

► The laws haven’t caught up with your work. It's no secret that technology evolves faster than the courts can keep up. This means that, if you're challenged on your work, there might be no precedent for how the courts should rule. In such a situation, your E&O policy would cover the cost of legal representation so you could defend yourself in court.

Why Do I Need Errors and Omissions Insurance?

Even if you're careful in all your work, have great relationships with your clients, and have never been sued in the past, it's still a wise idea to invest in an E and O policy.

Why? Imagine this scenario: you're an independent contractor and you're working on a project for a larger IT company. One of this company's clients is a multi-billion-dollar retailer. The project you're helping with involves updating the company's email system – pretty straightforward stuff. You do your work, the project ends, and everything's good.

But three months later, the company's email is invaded by a virus that compromises almost all the customer data the company holds. The company looks terrible and shoulders massive liability – and it's looking for someone to blame. Its team of corporate lawyers decides the best strategy is to sue everyone who was involved in any capacity with the email update – including you.

Even though you likely had nothing to do with the virus (and in fact, it was probably the fault of a poorly trained employee of the mega-corporation), you're now on the hook for presenting a legal defense for yourself. If you don't have an Errors & Omissions policy in place, the cash for lawyers' bills will have to come out of your pocket.
SHOULD EVERY IT FIRM HAVE ERRORS & OMISSIONS INSURANCE?

The short answer is yes. E&O is a must for every IT professional.

Beyond the perks outlined above, E & O coverage benefits IT professionals in these key ways:

► **It serves as personal protection.** Even as a careful independent contractor, you could be named in an E&O suit brought by a large corporate client related to a project you did minimal work on (as in the example above). Even if your involvement in the project was small, the cost of your legal defense could be enormous.

► **It helps win new clients.** E and O is not only useful in protecting your business against client claims. It can also help you land more clients. Carrying a robust Errors & Omissions policy demonstrates to clients that you have the resources necessary to serve it no matter what happens.

► **It protects you from mistakes (even when you’re not responsible).** Many IT experts think that they won’t make mistakes, probably because they have been in the business for years without a single unhappy client. But nobody’s perfect. E&O Insurance protects you whether your slipup or a mistake by an employee or contractor causes your client a loss.

► **It covers the gaps left by General Liability Insurance.** In the insurance world, “general” does not mean “comprehensive.” Your General Liability policy offers essential protection, but only against third-party claims of injury or property damage. If a client sues you over the work you did, your GL policy won’t pay for the suit. But your E&O policy will.

► **It protects you against frivolous claims.** Here’s a scary reality: even if you’ve done your work exactly as described in your contract, an unhappy client could sue you. While such a suit is unlikely to hold up in court, you’ll still be on the hook to present an initial defense of your business, which can cost thousands of dollars in lawyers’ bills and hours of your time. Having an E & O policy in place means you don’t have to worry about how the whims of unpredictable clients can hurt your bottom line.

**IMPORTANT NOTE:** Errors and Omissions Insurance works on a “claims-made” basis. This means that, in order to receive benefits, your policy must be active both when you file a claim and when the incident related to the claim occurs. In other words, if you start and stop E & O coverage with your individual contracts, you likely won’t have protection when you need it most.
QUESTIONS TO ASK YOUR AGENT ABOUT YOUR ERRORS AND OMissions POLICY

So how can you ensure that your Errors and Omissions Insurance policy is adequate for the risks your business currently faces? Call your insurance agent and ask these key questions:

► **Does my policy cover errors AND omissions?**
Be sure to read the fine print of your policy (or have your agent walk you through it). A policy with a lower premium may seem enticing, but reduced premiums often come with reduced coverage. Make sure that, if you decide to choose a cheaper policy, it doesn’t exclude coverage for work you expect to do.

► **What does my policy exclude?**
Policies that list exclusions typically offer more coverage than those that name covered incidents. Get to know the kinds of events and incidents that your Errors and Omissions Insurance doesn’t cover and update your policy if you start to offer services that might expose you to those risks.

► **Does my policy cover legal expenses?**
One major benefit of most Errors and Omissions policies is that they cover the legal costs (including lawyers’ fees) associated with defending a business against a claim. You may find a cheaper E and O policy that provides no legal defense coverage, but it’s probably not a wise investment. Legal bills are often the most expensive part of an E and O claim.

► **…but does it cover ALL of my legal expenses?**
To fully protect your business, make sure your defense coverage extends throughout the defense and appeals process. Otherwise, you could find yourself in the middle of court appeals with no legal representation – and no money to hire a lawyer.

► **Will my E&O policy provide me with a lawyer?**
Some policies provide legal counsel in the event of a lawsuit, which can save you the time and hassle of hunting down a lawyer who is both in your price range and familiar with handling E & O claims for small IT firms.

► **Is my insurer required to defend me against claims?**
Some E and O policies indicate that the insurer has the “right to defend” the insured, while others note that the insurer has the “right and duty” to defend. The “right and duty” clause offers you more protection, because it means your insurance provider is legally obligated to provide your defense if you’re sued.

► **What are my policy limits?**
Most policies have two limits: a per-occurrence limit and an aggregate limit. The occurrence limit is the maximum your insurance provider will pay to reimburse you for any single claim. The aggregate is the maximum it will pay for all claims in a year.

► **Are my contractors covered under my policy?**
Many Errors & Omissions policies extend coverage to 1099 contractors working with your company. This type of coverage is important if you work with contractors, as your company could be held liable for anyone doing work on your behalf.

► **Will I be covered even if the claims against me are groundless?**
In most cases, your Errors and Omissions policy will cover you whether or not the claims against you are well-founded. Check with your insurance agent for details about your policy.

► **Will my E&O track record affect my insurance rates?**
Often, maintaining a clean lawsuit record and taking certain precautionary measures (such as implementing good contracts practices) can translate to lower E and O premium prices.
WHAT ISN’T COVERED BY E&O INSURANCE?
Like any insurance policy, Errors & Omissions Insurance can’t protect your business against everything. While specific exclusions vary from carrier to carrier and policy to policy, the following are events that are commonly excluded from E and O protection.

► Malicious, dishonest, criminal, or illegal acts, including intentional violation of any law, regulation, statute, or ordinance.
► Services you might provide under the name of any other business, charity, or organization that is not named in the policy.
► Liability for damages against or on behalf of any other insured party named on the policy (i.e., if your partner sues you or your company, your policy won’t cover you).
► Copyright, patent, or trademark infringement.
► Bodily harm to any person, including sickness or death (though this may be covered by your General Liability Insurance).
► Damaged property or loss of use resulting from such damage.
► Libel or slander.
► Illegal discrimination.
► Violation of any securities act.
► Pollution.
► Humiliation, imprisonment, wrongful entry, eviction, invasion of privacy, or malicious prosecution.
► Insolvency.
► Extraordinary liability assumed under contract (unless the liability would have existed even in the absence of the contract).
► Failure to secure, provide, advise, or maintain financing or other monies (unless you have a financial services / investment advisor policy).

Keep in mind that, depending on your needs, you may be able to add coverage for some of these incidents to your E & O policy. The best way to ensure that your policy offers coverage for the risks you face is to talk with an insurance agent familiar with the needs of small IT businesses.

WHAT DOES ERRORS & OMISSIONS INSURANCE COST?

The cost of an E&O Insurance policy depends largely on the specifics of your business (number of employees, type of work you do, years of experience you have) and the deductible you choose (higher deductibles make for lower premiums and vice versa).

Below are rough ballpark estimates of what tech businesses of various sizes can expect to pay for a basic E and O policy. If, after you’ve read through this, you’d like to know what a policy would cost for your business, you can receive free customized quotes by completing our online insurance application.
Estimated Cost of an Errors and Omissions Insurance Policy for a Small Technology Consulting Company

For a small consulting firm with no more than two fulltime staff members, no more than 10 programmers, and between $250,000 and $1 million in annual revenue, here’s a rough estimate of the cost of E and O Insurance:

**Sample annual premium:** $2,500 – $4,500

- Sample deductible: $5,000
- Sample coverage limit (per occurrence): $1 million
- Sample coverage limit (annual aggregate): $1 million

**Note:** The policies used to generate these sample quotes include unauthorized access coverage and malicious code coverage but do NOT include coverage for intellectual property incidents.

Estimated Cost of an Errors and Omissions Insurance Policy for a Large Consulting Firm

For a large consulting company with six to 10 staff members, 10 to 50 programmers, and $3 to $10 million in annual revenue, here’s a rough estimate of the cost of Errors and Omissions Insurance:

**Sample annual premium:** $14,127

- Sample deductible: $5,000
- Sample coverage limit (per occurrence): $1 million
- Sample coverage limit (annual aggregate): $1 million

**Note:** The policy used to generate these samples includes coverage for unauthorized access coverage and malicious code coverage but does NOT include coverage for intellectual property liability. It’s also important to note that this policy includes a minimum earned premium of 30%, meaning that a business must pay at least 30% of the annual premium even if it decides to cancel the policy shortly after putting it in force.

Estimated Cost of an Errors and Omissions Insurance Policy for a Independent Contractor / Web Designer

For an independent contractor or sole proprietor who brings in no more than $150,000 in annual revenue, here’s a rough estimate of the cost of Errors & Omissions Insurance:

**Sample annual premium:** $1,000 – $1,500

- Sample coverage limit (per occurrence): $1 million
- Sample coverage limit (annual aggregate): $1 million

**Note:** The policies used to generate these quotes do NOT include unauthorized access or malicious code coverage. You may need these types of coverage if you offer security services such as firewall and antivirus application services. Including such protections in your policy might increase your premium by about 5 percent. Further, this quote does NOT include coverage for intellectual property liability.

Get Free Errors & Omissions Insurance Quotes for Your Business

If your business doesn’t fit neatly into one of these categories, don’t worry: you can receive free, customized quotes for Errors and Omissions Insurance policies by filling out an online insurance application.
HOW TO AVOID E&O CLAIMS

The U.S. Chamber of Commerce estimates that small businesses pay more than 80% of expenses associated with business lawsuits. Whether you’re a freelancer, an independent contractor, or the owner of a small business, you can’t ignore this number.

And even if you have an Errors and Omissions policy in place, an E & O claim can hurt you in three ways:

► Helping your lawyer prepare a defense for your business will eat up hours of your time.
► Having a claim on your record may increase your premium prices.
► A claim, regardless of its merits, can send a message to potential clients that you’re untrustworthy or careless with your work.

The following seven-step guide outlines strategies for minimizing the chances that you’ll ever have to make a claim on your E and O policy so that you can keep your business in the best financial shape possible.
7 STRATEGIES FOR REDUCING THE RISK OF AN E&O LAWSUIT

1. **Over-communicate with clients.** Knowing exactly what your customers want can be difficult because of the IT-layman communication gap. Your clients understand the results they want but don’t have the technical expertise to know how to get them. You have that expertise, but may not be clear on your client’s vision. When in doubt, over-communicate, ask questions to verify, and check in at various points of a project to ensure you’re on the right track.

2. **Actively manage deadlines.** One of the biggest challenges for IT pros is estimating and meeting deadlines. Customizing software, for example, can be incredibly complicated and difficult. A client’s preexisting IT infrastructure, the regulations in their industry, and the structure of their company will complicate your task.

3. **Warn clients about delays.** If you do miss a deadline, keep your clients in the loop. Should you hit a road bump in development, inform them if you think it might cause a delay. This lets them plan ahead to avoid losses of productivity.

4. **Test software iteratively.** It may seem like more work, but because iterative testing helps nip problems in the bud, software engineers often find it saves them time in the long run.

5. **Use contracts that pass legal muster.** Contracts help define the limits of your liability and clarify your responsibilities in a project or business relationship. But not all contracts are created equal. Make sure the contracts you use (especially for hiring freelance or 1099 workers) have been approved by a lawyer so you know they’ll hold up in court. Hiring a lawyer can be costly, but you may be able to save money by having an attorney approve a few template contracts that you can adapt over and over again.

6. **Build strong customer relationships.** It’s a cliché that business is built on personal relationships – but it’s true. Being friendly and professional with clients ensures clear communication. Strong customer relationships prevent misunderstandings that can lead to lawsuits.

7. ** Educate your clients.** With a third of all data breaches caused by employee errors, it’s vital that you educate your clients on data security. Remember that you can be sued for a data breach even when a client is responsible.

It shouldn’t surprise you that these tips are about doing your job well. What might surprise you is how many of them have to do with client relationships. Communication and education are nearly as important as the choices you make about software and hardware. Understanding the personal aspects of your business as well as the technical is a key part of avoiding Errors and Omissions lawsuits.

3 MOST COMMON ERRORS & OMISSIONS CLAIMS FOR TECHNOLOGY FIRMS

These three incidents are among those that most commonly cause IT freelancers, contractors, and small-business owners to file claims on their E and O policies.

1. **Client data breach:** As an IT professional, you likely provide your clients with products and services that involve the handling, storing, or processing of digital data. If one of your clients experiences a data breach, they may be able to sue your business to recover some of the expenses of responding to the breach. Luckily, most Errors and Omissions policies sold to IT firms include protection for data breach lawsuits (called third-party Cyber Liability Insurance).

2. **Breach of contract:** You fail to live up to the terms of a project laid out in a contract, and your client suffers a loss, which prompts them to sue to recover damages. Be aware that a breach of contract suit can be over something as small as missing a deadline.

3. **Negligence:** You, an employee, or a contractor fails to use “reasonable care” (or your client believes you did). Either way, the work you did causes losses for your client. To recover those losses, your client sues.

Any of these incidents can trigger an E&O claim that leads to an expensive and time-consuming lawsuit. E and O policies for IT professionals cover the legal expenses associated with defending your business in such a lawsuit.
3 TIPS FOR RECEIVING E & O INSURANCE PAYOUTS EVERY TIME

To smooth the claims process and maximize your odds of receiving E & O benefits in a timely manner, follow these three steps.

1. **Know what counts as a claim.** Here’s something that comes as a surprise to many IT business owners (and what causes some to have their claims denied): “claim” doesn’t necessarily mean “lawsuit.” In fact, many Errors & Omissions policies define a claim as any oral or written notification of an event that might lead to a lawsuit. That means you need to notify your insurance provider as soon as a client mentions that they’re dissatisfied with your work, especially if they mention suffering a financial loss or contemplating legal action.

2. **Report claims quickly.** Many E&O policies only offer coverage if you report a claim in the same policy period that it was filed. Here’s what that means: Imagine that, at the end of 2013, a client emailed you insisting you breached contract by missing a deadline. Your policy covered 2013, and you’ve renewed it for another year. Months later, the client brings a lawsuit against you in early 2014. When you submit the claim to your insurance provider, it might not cover you unless you already submitted notification about the initial email. Why? Because some E&O policies work on a “claims made and reported” basis, meaning that coverage is only available to those who report claims immediately (i.e., within the same coverage period as they were introduced). Yes, this is fairly complicated. Be sure to ask your agent to clarify exactly what you need to do to receive E&O benefits from your policy.

3. **Update your policy as needed.** Many insurance providers adjust their products (i.e., insurance policies) from year to year. And it’s common for a small technology business to undergo fairly significant changes in the course of a year. Whenever you add new services, hire new employees, or otherwise change the way you do business, be sure to contact your agent to see if your E&O policy needs to be adjusted.

CONCLUSION

As an IT freelancer, independent contractor, or technology business owner, you’re in an excellent position to help people improve their lives and their businesses by implementing the latest technological solutions. To make sure your business also benefits, it’s essential to actively manage the risks that threaten your revenue. For IT professionals, risk management should include testing, client communication (including client education), contract use, and maintenance of business insurance.
ABOUT TECHINSURANCE

Techinsurance offers customized business insurance to small and micro businesses in the U.S. By providing a streamlined online application process and agents with expertise in a variety of technology and IT fields, TechInsurance enables an insurance-buying process unlike anything else on the web. Customers enjoy the convenience of comparing policies online and the security of working with a dedicated agent who can answer their questions and find policies that match their risk exposures and budgets. Since its founding in 1997, TechInsurance has served more than 150,000 of America’s small businesses. It has offices in Chicago and Allen, Texas.

CONTACT US

When you’re ready for a fast, reliable quote for your small business insurance needs, give us a call or send us an email. Whether you have a question about our company or your coverage needs, we’re ready to help!

1301 Central Expy. South, Suite 115
Allen, TX 75013

voice [toll free] 800-688-7020

© 2014. TechInsurance is America’s #1 online insurance agent for computer, web and IT professionals, including the self-employed and small businesses with 10 or fewer employees. TechInsurance allows IT businesses to apply for insurance coverage and receive multiple quotes from leading insurance carriers, including CNA, Zurich, The Hartford, Philadelphia, Travelers, ACE, USLI, and Hiscox. We offer business owners a variety of insurance protections, including General Liability Insurance, Professional Liability Insurance, Errors & Omissions Insurance, Umbrella Insurance, Workers’ Compensation Insurance, Fidelity Bonds, and more.

TechInsurance.com

Photos: (Unless otherwise indicated, all images are copyright of Shutterstock, Inc.)
Cover Photo copyright: Veer.com a Corbis Copyright Agent

TIGEB-2-20-2014