optimalnetworks®

Law Firms & Cybersecurity

WILL YOUR FIRM BE THE NEXT HEADLINE?

Feel like you can't go a day without hearing "XYZ Company was hacked"? It's an exaggeration, but not by much—cyberattacks are increasing with no apparent downturn in sight.

optimalnetworks

What is your firm doing to protect itself?

Firms like yours don't have an option when it comes to keeping client data secure; you are obligated to keep your clients' data confidential, no ifs, ands, or buts about any of it.

So, how can you get your firm on the right path toward robust and comprehensive cybersecurity?

In this brief I'll walk you through:

1. The top security risks for your law firm
2. How you can best protect yourself from damaging malware
3. What all these protective measures will actually cost your firm in the long run

If at any point along the way you have a question, you can find my contact information below my signature.

Best,

Heinan Landa
CEO, Optimal Networks
Mail: hlanda@optimalnetworks.com
Phone: 240.499.7905

What are the Top Cybersecurity Threats to Law Firms?

My law firm clients are scared—and they should be. It's a scary, data-filled world and they want to know how Optimal recommends protecting that data. They also want to know what exactly it is they should be scared of: what are the top cybersecurity threats to law firms?

Given that in 2014 cybercrime incidences increased by 10.4% over 2013 numbers*, I spend a lot of time strategically advising my clients about how to protect their networks. (In fact, I've been asked about this so many times that cybersecurity took the #1 slot in my firm's biannual tech trends brief this past February.)

Organized hackers are seeking high-reputation and resource-rich assets. And they are targeting law firms with a vengeance because access to law firm data is hitting the data jackpot.

WHAT ARE CYBERCRIMINALS AFTER WHEN THEY TARGET LAW FIRMS?

Why are you at risk? Because your firm has one or more of these sitting on your servers:

- **Patent and insider deal (M&A) information**
- **Healthcare data**
- **Case and/or litigation strategy information**
- **Confidential client business trajectory information**
- **Attorney-client privileged communications**
- **Personally Identifiable Information (PII) for employees, clients, and vendors**
- **Financial information, including credit card numbers and PIN numbers.**

2014
CYBERCRIME INCREASED
10.4%

By far the largest threats to the security of law firms live **within the firms themselves**; not prioritizing data and network security, and having insufficient security measures and policies in place is what really makes firms vulnerable to attack.

WHAT ARE THE TOP CYBERSECURITY THREATS TO LAW FIRMS?

By far the largest threats to the security of law firms live within the firms themselves; not prioritizing data and network security, and having insufficient security measures and policies in place is what really makes firms vulnerable to attack.

In Cisco Systems Inc.'s 2015 Annual Security Report, law firms were ranked as the seventh most-vulnerable industry. However, many law firms don't yet appear to appreciate that they are popular targets.

Take a look at the results from a 2013 International Legal Technology Association (ILTA) survey and you'll see what I mean:

- **76% of law firms surveyed did not require two-factor identification**
- **72% did not issue encrypted USB drives**
- **64% did not automatically encrypt content-based emails**
- **56% did not encrypt laptops**
- **90% did not employ any laptop tracking technology**
- **64% had no intrusion prevention tools in place.**

It's precisely these kind of oversights that can lead to compromised data, and all of the repercussions therein; without any preventive measures in place, you are all but asking for your firm to be infected by malware, or for hackers to intercept your sensitive data with next to no effort.

What can law firms do to better protect themselves?
Make cybersecurity a top firm priority. Know that you are now the target—and that the attack can come from across the world or across the hall. In other words, give security a seat at the partner's table; without a full commitment to bolstering your defenses, there's no way your firm will make any progress.

A 2013 ILTA SURVEY REPORTS

- **76%** of law firms surveyed did not require **two-factor** identification
- **72%** did not issue **encrypted USB** drives
- **64%** did not automatically **encrypt content-based** emails
- **56%** did not **encrypt** laptops
- **90%** did not employ any **laptop tracking** technology
- **64%** had no **intrusion prevention tools** in place.

From there, take a good hard look at your existing security measure and policies, and ask yourself if they are truly sufficient. Do your policies address system usage and access, and ways to manage change? Do they provide an audit trail for you organization? Do they dictate how to handle an employee leaving or being terminated?

Evaluate your current security elements and policies by asking:

- **What do we intend to protect?**
- **How are these elements being protected?**
- **Do our policies and operations support the protection of these elements?**

From comprehensive firm-wide data security policies to regular security audits, preparation is the secret weapon when battling cybercrime.

To help you get started down this path, my next article will take a more concrete, tactical look at how you can protect your firm from one of the most pernicious threats out there: malware. I'll zero in on the different types, how to keep your attorneys and staff educated about how to prevent infection, and how to make sure your IT systems are set up to keep your data safe.

**The Ponemon Institute's 2014 Global Report on the Cost of Cybercrime*

The Best Ways to Prevent Malware for Law Firms

Did you know that in Cisco Systems Inc.'s 2015 Annual Security Report, law firms were ranked as the seventh most-vulnerable industry? That's scary, considering how heavily law firms rely on data, and how heavily their clients rely on privacy.

Even if you've successfully given cybersecurity a seat at your partner's table, the efforts can't end there; now we must shift our attention to what specific actions your firm needs to take to keep your data safe once the importance has been established.

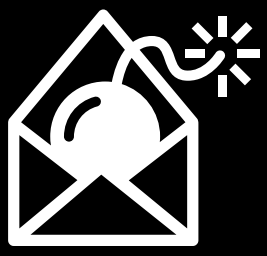
To do this, I'll spend this article digging into malware, how it can impact your firm, and how you should ultimately leverage both technology and policy to prevent things like ransomware and spyware from compromising your client documents—or worse.

HOW IS MALWARE PUTTING YOUR LAW FIRM AT RISK?

What exactly is malware, and how can it affect your firm's data? Here are some quick definitions:

- **Malware** is actually not a specific threat itself, but rather a blanket term that encompasses any software that gets installed on your machine to perform unwanted tasks for a third party's benefit. Spyware, viruses, and ransomware are all forms of malware.

- **Viruses** are types of software that can self-replicate and spread to other computers on your network—hence them being likened to an infection. Viruses are programmed to damage a computer by deleting files, reformatting a hard drive, or using up computer memory.



CRYPTOLOCKER

FIRST

FORM OF RANSOMWARE

SEPT '13

Files are encrypted until you pay a certain price—and the only way around it (without paying) is to restore a backup of your data.

Without a disaster recovery solution, the consequences can be devastating to your operations and reputation.

> **Spyware** is software that gathers information from your computer, data, and system, and transmits it to interested parties. I'm talking your web history, browser and system information, and IP addresses. Advanced spyware can even monitor your keyboard for any personally identifiable information (PII). For an industry that necessarily deals with privileged information, this brand of malware is quite troublesome.

> **Ransomware** is a type of software that hackers use to hold individuals' data hostage until they pay for its release. CryptoLocker, the first form of ransomware, appeared in September 2013 and circulated by way of infected email attachments. Here, your files are encrypted until you pay a certain price—and the only way around it (without paying) is to restore a backup of your data. I've seen ransomware hit law firms, and if not for their disaster recovery solution, the consequences could have been devastating to their operations and reputation alike.

THE BEST WAYS TO PREVENT MALWARE FOR LAW FIRMS

Here are a few of the best ways to protect your firm from malware. As you'll see, not all of these solutions are technical in nature.

> **Keep anti-virus and anti-malware up-to-date.** Sure, almost all law firms have this software in place. But is it being updated on a continual, consistent basis? Your protection is only as good as your maintenance.

> **Have a good spam filter in place.** You can prevent high-risk emails from touching your Inbox in the first place by implementing a robust spam filtering solution.

> **Keep your operating systems, firewalls, and firmware up-to-date.** Are your servers and workstations running operating systems that are still being supported? Is your

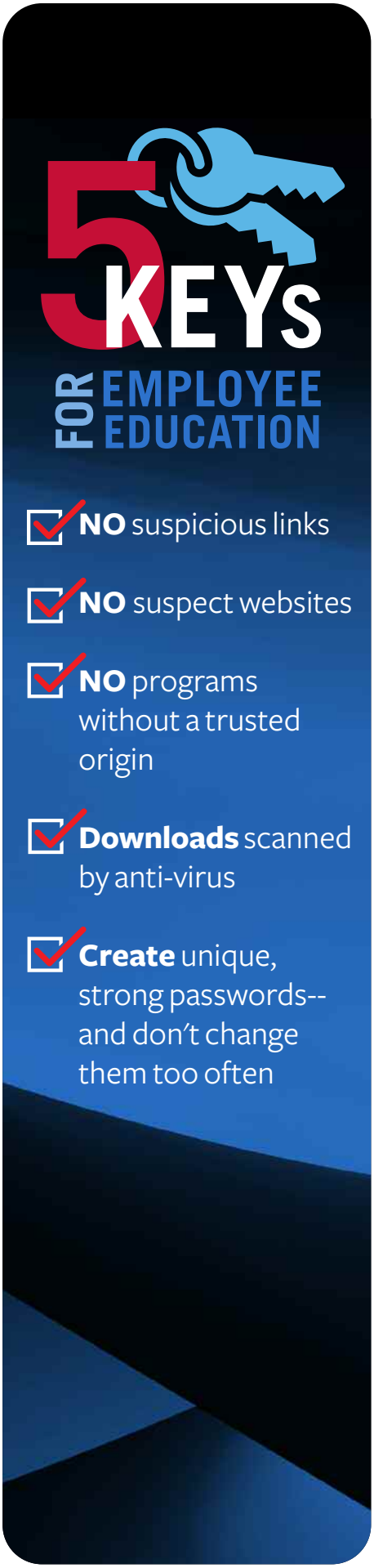
firewall current? Is everything being automatically updated and patched on a consistent basis? What about your firmware? It is important that these elements stay current to protect against evolving threats.

> **Create and enforce password policies.** Good, difficult-to-guess passwords are essential to computer security. What makes a strong password? In a nutshell, they (1) are at least eight characters long; (2) include letters, numbers, special characters and capitalization; and (3) are changed infrequently. Create a company policy that outlines these tips, and hold attorneys and staff to it. (Have a fussy partner? Get them a password manager before you let them off the hook.)

> **Create and enforce an equipment use policy.** Set boundaries as far as what your attorneys and staff are permitted to do on company-owned equipment. To what extent can they use things like laptops and phones for personal purposes? Can they install software of their choosing? Will there be mandatory scans, backups, or encryption? Establish clear rules, and wrap them into your onboarding process.

> **Create and enforce an employee separation policy.** Is your firm doing anything to ensure that access to your network is effectively revoked immediately upon an employee's departure? When an employee leaves—whether they're a partner, attorney, paralegal, or support staff member—this termination policy must be enforced so that disgruntled former employees cannot introduce malware to your system or access confidential data.

> **Educate employees.** This is the kicker. An essential part of practicing secure computing is educating employees to make smart computing decisions. For example, what would folks inside your firm do if someone called and asked for their social security number? Create regular, security training sessions for your employees that cover security basics, including:



- **Avoid clicking on suspicious links in emails**
- **Avoid going to suspect websites**
- **Ensure all downloads are automatically scanned by anti-virus**
- **Create unique, strong passwords—and don't change them too often**
- **Do not run programs from which you cannot identify an origin**

In today's world, we all must prepare in order to protect our business. Once you establish the basics (investing in a robust anti-malware software), create comprehensive policies and user training programs to round out your anti-malware efforts.

Beyond that, I also strongly recommend periodic security audits as a way to keep your firm secure. After all, the best way to make sure you've remediated all existing vulnerabilities is to have an outside resource *actively prod your systems for vulnerabilities*. Your provider will run scans, they'll analyze your existing policies, and they'll set forth prioritized recommendations to reinforce any weaknesses.

True, this all is an investment of time and money that you may not feel your firm has to spare.

In fact, I often find that cybersecurity takes a back seat in the name of "limited funds" or "budgetary restrictions" or some other incarnation of "I don't want to spend this kind of money."

This is why I wanted to spend some time talking numbers; when it comes down to it, how much should you actually expect to invest in IT security?

I'll walk you through it.

How Much Should Law Firms Spend on IT Security?

Let's take another look at the results from that 2013 ILTA survey:

- **76% of law firms surveyed did not require two-factor identification**
- **72% did not issue encrypted USB drives**
- **64% did not automatically encrypt content-based emails**
- **56% did not encrypt laptops**
- **90% did not employ any laptop tracking technology**
- **64% had no intrusion prevention tools in place.**

In the legal space, ethics dictates that client data is sacred, yet—ironically—firms are too often taking insufficient measures to actually protect this data.

So, what kind of investment is it going to take to shore up your firm's security and to keep your data secure on an ongoing basis? This is a question I've gotten over and over again from my law firm clients, and while the answer is complex, it's one I'm always happy to explore.

Below I'll work through the main factors that will affect what your firm's overall IT security investment will look like, and what you should expect to see in the long run.

KEY FACTORS THAT INFLUENCE THE NATURE OF YOUR IT SECURITY SPEND

The amount you want to invest in your law firm's IT security each year depends on the following factors:

- **Whether or not you've had a recent security audit.** Before you can make any strides toward bolstering your IT systems, you have to establish a clear baseline. This takes

In the legal space, **ethics dictates that client data is sacred**, yet—ironically—firms are too often taking insufficient measures to actually **protect this data**.

How secure do you want your firm to be?

Would even the slightest breach tarnish your reputation for good?

Do you trust your attorneys and staff to follow best practices without any mandated controls in place?

As you can probably guess, the **lower your tolerance, the higher your costs will be.**

the form of an outside provider performing an objective gap analysis that locates existing vulnerabilities in your environment, and offers a roadmap for remediation. (Put simply, if you haven't invested in a security audit recently, you'll need to.)

> **The size and complexity of your firm.** The more nooks and crannies your technology environment has, the more effort (and likely money) it's going to take to secure them. Not only that, but a larger size count also means investing more time in properly training your attorneys and staff on your internal security policies.

> **The state of your current hardware and software.** Are your servers and workstations regularly patched and monitored for health statistics? Are any of your servers out of warranty? Are you running machines with Windows XP that is no longer supported in any capacity? Is your software patched and properly licensed? If you are working off of an aging infrastructure, you will likely have substantial up-front costs to upgrade.

> **The nature of your data.** The vast majority of your firm's data is going to consist of privileged information. Still, depending on your firm's specific area(s) of practice, your particular data might range from moderately sensitive, to completely and utterly confidential. Ask yourself this: if your data were to get in the wrong hands, what would the repercussions be? The more tightly you need to control your data, the more you'll need to invest.

> **Your tolerance for risk.** In the end, how secure do you want your firm to be? Would even the slightest breach tarnish your reputation for good? Do you trust your attorneys and staff to follow best practices without any mandated controls in place? As you can probably guess, the lower your tolerance, the higher your costs will be.

HOW MUCH SHOULD LAW FIRMS SPEND ON IT SECURITY?

As you can see from the factors above, there is an adoption curve when it comes to security. As a general rule, your placement on this curve is going to dictate the nature of your overall IT security spend.

In other words, if you are just now taking the initiative to secure your firm, you're going to have to invest a significantly higher up-front amount than those firms that have been making security a priority and an integral part of their culture for quite some time.

A security audit on its own, for example, is going to run you between $20,000 and $30,000 on average given the complexity that is inherent to law firms.

From there, you could be looking at an investment of $10,000 to $15,000 each year to implement any necessary technology solutions, and to test and make adjustments to them on an ongoing basis.

This, of course, is only a ballpark—if your assessment uncovers $40,000 worth of vulnerabilities in your current environment, and if you value the safety of your data, you really need to spend whatever is necessary to protect your clients and your reputation.

Across the board, the consequences of a successful attack on your firm can be devastating to the point where your entire business is crippled. So if I'm to offer any one piece of advice, it's that you need to work with a trusted resource to identify the appropriate solutions and next steps for your firm, and that you need to find a way to implement and maintain them no matter what.

Can you really afford not to?

There's an adoption curve when it comes to security, and your placement on this curve **will dictate your investment.**

Security should have its own dedicated budget within your firm, separate from your overall IT spend.

No matter what Heinan is up to, he maintains a firm grounding in **both steadfast ethics and good old fashioned fun.**

What Heinan Does

Heinan has been President and CEO of Optimal Networks, Inc., since he founded the company in one of his parents' vacant offices back in 1991.

Before then, he kept himself busy earning a BS and MS in Electrical Engineering and Computer Science from Johns Hopkins, and an MBA from Wharton.

Today, when he's not talking through the latest technology trends with Optimal clients, writing for the American City Business Journals or Legal Management, or serving as VP and CTO of the Wharton Alumni Club of Washington DC, you'll probably find him running sound for his son Adam's band, sipping tea with his daughter Shari, or attending one of his wife Melissa's presentations at the University of Maryland.

No matter what he's up to, he maintains a firm grounding in both steadfast ethics and good old fashioned fun.

What Optimal Networks Does

Optimal Networks, Inc., based in Rockville, Maryland, has been providing technology support to the law firm community for the past 24 years. Over these years, we have gained extensive insight into the unique technology needs of law firms, and what tools and resources need to be in place for their systems to be truly effective.

We've put this experience into practice in the form of DMS selection and implementation projects, disaster recovery/business continuity plans, general ongoing managed IT services, and highly-customized cloud computing environments that support critical line-of-business applications such as iManage, iScrub, Time Matters, and Quickbooks.

Across the board, our approach to IT is unique in our ability to capture the business goals of our client, and fit the most appropriate technologies to support those goals.

We currently have over 35 full-time staff members in Maryland, Pennsylvania, and North Carolina, all of whom operate with a fierce commitment to honesty, to premium client service, and to taking the anxiety out of IT.

We've put our **experience into practice** in the form of DMS selection and implementation projects, disaster recovery/business continuity plans, general ongoing managed IT services, and highly-customized cloud computing environments.

What Frank Schipani of Gilbert, LLP Says Optimal Does

A 28-attorney law firm with a four-person IT department must be serious about technology—not just as a utility, but also as a key business facilitator and valuable resource.

Frank Schipani, Director of Information Technology for Gilbert, LLP, a Washington, DC-based law firm focused on strategic risk and litigation consulting and insurance recovery, understands his team's role in no uncertain terms:

"In order for the IT team to leverage technology to help the firm grow, we need to engage with the business side of the firm, which takes time," says Schipani. "Having a company like Optimal Networks to run our day-to-day technology allows my team and me to understand the firm's needs from a business perspective and utilize the technology accordingly."

HIGH VALUE TECHNOLOGY: A HIGH-INTEGRITY APPROACH

"You can tell pretty quickly when a company places your interests first or their own," says Schipani.

"Optimal established a level of trust immediately in three ways: demonstrating technical expertise; doing what they say they're going to do; and not always looking to sell us the latest technology, just because it's available. This level of trust is critical because it means I can truly treat them as an extension of my staff—and one that doesn't need much direction because they really get our business and the way we work."

"Optimal establishes **a level of trust** immediately in three ways: **demonstrating technical expertise**; **doing what they say they're going to do**; **and not always looking to sell us the latest technology, just because it's available.**"

IT AS AN INVESTMENT VS. COST CENTER

"It is no longer acceptable for the IT function to just keep the lights on," continues Schipani.

"Sure, there's a part of IT that's a utility—a necessary cost. But if you're spending all your time on that then you're obsolete. IT has to help move the organization forward and identify areas where they can drive value."

INFORMATION TECHNOLOGY MOVES UP THE BUSINESS VALUE CHAIN

"Frank Schipani, Gilbert's IT Director, made it pretty clear at the onset that he needed help reducing his team's load so they could focus more on addressing business challenges beyond day-to-day IT," says Chris Abel, Optimal's Manager of Consulting Services. He continued, "Optimal is here to provide a deep pool of resources that Schipani can draw on at any time to address areas where his internal IT staff may be limited. We act as an extension of his team, an extension of expertise, and that is a competitive advantage."

"Sure, there's a part of IT that's a utility—**a necessary cost**.

But if you're spending all your time on that then you're obsolete.

IT has to help move the organization forward and identify areas where they **can drive value**."