CLIENT

BILL OF RIGHTS

We at TOSS C3, are committed to delivering Excellence. Our clients receive the absolute best technology solutions, services and support possible. To that end, we pledge to deliver the following rights to all our clients, and would suggest you DEMAND this same level of service, honesty and integrity from any IT vendor you choose.

You have a right to expect fast response and resolution on any IT-related problem you are experiencing. We pledge to respond to your request for help within 15 minutes or less during the workweek, and within 1 hour on weekends and evenings. We also pledge to show up to our scheduled appointments on time, and to give you as much advance notice as possible when we cannot be there as promised due to a circumstance beyond our control.

You have the right to get answers to your questions in PLAIN ENGLISH. We pledge to never use "geek speak" or talk down to our clients regarding an IT-related topic.

You have a right to expect exceptional services from friendly people who appreciate you as a client. We pledge to always treat you and your team with the utmost level of courtesy, professionalism, and respect at all times.

You have a right to expect us to lead the way in looking for new and innovative technologies to improve your profitability and productivity, and to protect your business assets. We pledge to stay on the leading edge of cybersecurity, cloud technologies, compliance, and office productivity tools so you are always presented with the best-in-class options.

You have a right to individual attention and to know who is touching your computer network and data. We pledge to never outsource your support to a third-party company. You will always have a dedicated account manager and support team who know you, your company, and your preferences.

You have a right to understand every aspect of your IT assets. We pledge to provide full and complete documentation of all hardware and software assets, data and systems, as well as complete password control, so you never feel as though you are "held hostage" by your IT company.

You have the right to receive accurate invoices. We pledge to always deliver on time and on budget, and never surprise you with hidden fees, extras and overages that you have not agreed to.

You have the right to be protected against our mistakes and failures. We pledge to maintain error and omissions insurance, as well as workers' compensation, cyber liability, and business liability, in the unprecedented event of a mistake on our part.

You have the right to know the status of your account and support requests, no matter what time of day or night. We pledge to provide secure access to status reports via our Help Desk System 24 hours a day, seven days a week, and to communicate the progress of resolving any issue. You will never have to manage us or remind us of promises we've made.

You have the right to a quarterly, semi-annually or annual business review. Whichever frequency is best to help us keep your technology in line with your business strategies and goals.

TOSS is a *By Referral Only* business. Referrals come to us from happy, satisfied clients. We want you to recommend us, and we know that will only happen if you are thrilled with our service. That is why we work tirelessly to go above and beyond the call of duty. The establishment of our Client Bill of Rights, along with our continual and substantial investment in people, processes and technology, clearly demonstrate our commitment to our clients.

TOSS C3
Cybersecurity | Cloud | Compliance

+1.888.884.8677 | info@toss3.com

29 Reasons Why You'll Want To Work With TOSS C3 Over Any And Every Other Technology Company

(888) 966-9514
www.TOSSc3.com

What Our Clients Are Saying About Us

Robert Cohen, CPA
KWC Partners, LLP

We Do Not Let Our Employees Use Any Application Outside Of The TOSS C3 Cloud

We no longer have to go through hoops to get something fixed on a very timely basis. We had used a different company which was located in California and the time difference was a killer. If we had a problem when we came in, we could not reach them until it was 9 a.m. on the West Coast. We utilize TOSS C3 to update all of our applications and this is always done in a timely fasion. We believe that TOSS C3 kept us from cyber security issues, and there are no problems getting into the cloud. We use TOSS C3 when visiting clients all over the USA and when some of our people go to Japan.

Alex Fuchs,
IT Manager
The Paper Store

Few MSP's Are Able To Offer The Variety Of In House Hosted Solutions That TOSS Can

Working with TOSS has brought with it a wealth of highly qualified technical resources that are subject matter experts in a wide variety of fields. The Senior Engineers at TOSS in particular have resolved issues where other engineering resources have failed. When you utilize TOSS C3 solutions in their private cloud they own the support experience around those initiatives. This was particularly helpful for us when deploying DaaS (Desktop as a Service) in our environment. Our retail footprint utilize DaaS heavily and TOSS engineers support every aspect of that environment.

TOSS is uniquely positioned as a leader in the private cloud and the DaaS space. Few MSP's are able to offer the variety of in house hosted solutions that TOSS can while also maintaining seasoned engineering resources for support needs.

TOSS C3 Is The Best Decision And Investment I Have Made In Our IT Environment

Daniel Rivera,
Chief Technology Officer
JSH Properties Inc.

I understand that pricing is a huge concern. However, when selecting an IT company cheaper is never better. Small startups offer lower pricing, but in return you won't get the same quality of service, the experienced staff and the 24/7 support that you get from TOSS C3. They have a full team of IT professionals willing to help you any way they can, and they pride themselves on their quality of service. I always feel that if you pay a little more for better service you can't go wrong regardless of the price tag. IT is an important structure in a business. Every business focuses and relies on their technology to operate. I feel that if you go with TOSS C3 you will be just as happy as I am with that decision.

You Need To Compare Apples To Apples When Shopping For An IT Firm

Glen DeRosa,
M.I.S. Director
City of Revere

Things such as redundancy for backups and continuity of service in all instances are especially important if you cannot afford to be down for a long period of time. You need to factor in total cost of down time including idle staff whom you are still paying. Sometimes the dollar you save will cost you 10 times as much in the long run. You will also want a proactive monitoring solution in place to avoid any potential data breach. Take a look at recent statistics on how many ID thefts there are daily. Someone could infiltrate your network to take just basic personal information and you may never know. Worst case, your client data is stolen and held for ransom while you are trying to do business. Then what?

Jim Hachey,
President
In-Building Cellular

We've Been With TOSS C3 For 18 Years And On The Cloud For Five Years And We've Never Lost Data

If you are not monitoring your system every day, it can all go away. The IT world is getting more and more hostile. As a business, we can't keep up with the latest spam, malware and viruses but TOSS C3 can and does. TOSS C3 has been monitoring our system and protecting us from spam for years. We've never lost data, we've never had a serious virus, and we've never had anyones identity stolen. Running our IT system is the least of our worries due to the cloud and TOSS C3's protections. In addition, we can get on our system 24/7 anywhere, anytime. Peace of mind.

Denise Green,
Financial Director
Mackie Shea, PC

It Reduces My Stress Knowing My Business IT Security Is Not Something I Have To Pay Attention To

Many IT companies hire new people and have a lot of turnover. With TOSS C3, my experience is that the IT staff gets to know us and vice-versa, and the response we get is more reliable because we are not re-explaining everything all the time. I believe that continuity of employees is a sign of a good company that treats employees well and can be counted on to be there for me over time, which TOSS C3 has been and I count on them being there for me in the future. Knowing, with confidence, that no one in my company has to monitor all the systems involved in running our business is a way to let the rest of us do what we were hired to do rather than spending time on add-on duties.

John Horne,
VP Information Technology
Associated Industries of Massachusetts

Reliability, Predictability, Professionalism, And Trust Are The Key Elements Of Any Business Relationship

We've been with TOSS C3 for many years. I get regular calls and emails from other IT consultants wanting to earn my business. My reply is always 'when I become dissatisfied with my current IT service provider I'll open the door to new IT consultants.' That hasn't happened. I rely on TOSS C3 to keep our IT environment running. The core team at TOSS C3 has been around for as long as we've been working together. It's hard to put a price on that.

George Hall,
Partner
Anderson & Krieger, LLP

I Can't Speak To What The Competition May Be Offering, Because It Hasn't Occurred To Us To Shop Around. It's The Best Technology Decision We Ever Made

A great test of virtues of TOSS C3 was when we moved from Cambridge to Boston a couple of months ago. Our network was never down, and many of us continued working from home seamlessly as everything was crated up and moved over here. Our desktops were just plugged in and ready to go on Monday morning, because all we needed was Internet access. We can move all we want, and work from wherever we want, because our network never needs to move. The move was also a good demonstration that, when we do need on-site support, TOSS C3's staff has been here in whatever numbers are necessary to get the job done quickly and professionally.

Susan Sawyer,
Firm Administrator
Tucker, Saltzman,
Dyer & O'Connell, LLP

Cloud Computing Levels The IT Playing Field

With aging equipment and outdated software, we knew we were facing a BIG cash expenditure to get updated. TOSS C3 presented us with the perfect solution in IT as a Utility ®. After one demo, we knew we had to have it and that we were ready for a change that would make us current and increase our competitiveness. In December 2012, our law firm changed from in-house servers to TOSS C3's cloud based platform. We also upgraded our email and word processing software. Oh, and it all had to happen over the last few days of the year so we could be live January 1st. TOSS C3 handled everything seamlessly. Our cloud system enables remote access much greater in speed and reliability than anything we have ever used before. The TOSS C3 Cloud has saved us well over $67,000 in IT expenses and lost productivity so far. For small law firms, cloud computing levels the IT playing field, and TOSS C3 clearly has the skill necessary for proper planning and implementation.

Judy Griffin,
Fund Benefit
Administrator
Cambridge Public
Employees Dental
& Vision Fund

Finding A Company That Is Willing To Work With Such A Small Employee Base Was Very Hard To Find, And TOSS C3 Treats Each Client The Same

To let you know a little about our company, we are very small - two to four employees at the most. Having a company that treats even the smallest clients like they treat every other larger company is very hard to find. Based on our experience, no client is more important than the other at TOSS C3. We've worked with other companies that were great at first, then towards the end were horrible as far as response time, calling back, caring about our business needs, and IT experience. With TOSS C3 you get a response quickly and a person to talk to, and their IT people speak in a way that's not so technical you can't understand.

Chris Riley,
President & CEO
Community Service Stations

Data Backup And Disaster Recovery Is Automatic

Prior to implementing TOSS C3's IT as a Utility®, we never backed up crucial spreadsheets and documents. Now this happens automatically without us needing to do anything which is a great relief. All our Microsoft and Linux applications are offsite in the cloud, so we are able to access them from the office or from any remote location. The part I like the most abouit the remote access is that whether I use a desktop, laptop, or iPad, the experience is the same and it's fast. The support from TOSS C3 is friendly and fast; 10 minutes or less. Overall, going into the cloud with TOSS C3 is the best IT business decision I've made.

HASSETT & DONNELLY
ATTORNEYS AT LAW

Nancy Brodeur,
Office Administrator
Hassett & Donnelly, P.C.

Working With TOSS C3 Has Created A Reliable Network Which Has Benefited Our Clientele As Well

Without 24/7 monitoring you could come in on Monday morning and basically be down for who knows how long. The benefit of this is that someone is there to fix any alerts that may cause your network to go down and can fix them even before you walk in the door the next morning. I can't say enough about the reliability. As for the backup systems, we used to do it manually and took tapes off site. With that comes security concerns; you have to remember to run the backup but you never really know if the backup actually ran correctly. With the backup system TOSS C3 recommends, and that we fully endorse, I no longer have to worry if the backup ran properly and I know the information is safe and secure. I also know that should something occur on site to our hardware we could be back up and running again in a short period of time having the additional backup in the cloud.

Paul Masuret,
Executive Director
Casner & Edwards, LLP

I Save Tens Of Thousands Of Dollars Per Year With TOSS C3

TOSS C3 fully covers all of my network and IT systems issues and saves me the expense of having to maintain it all myself. TOSS C3 also handles all of my network back up and disaster recovery, both at my office and at their remote cloud data centers. Their staff is professional, knowledgeable, efficient, and nice to work with. There have been a number of weekend issues that have come up and TOSS C3 has always been there to resolve these issues. Even when I call at 7 a.m. on a Sunday morning or a Friday night, they are always quick to respond and get the issue resolved. I remember one time, when the building's electricity shut down, TOSS C3 noticed we had lost service. Their engineer contacted me, and he drove down to Boston and made sure everything was working and back up and running properly. Bottom line, I save many tens of thousands of dollars per year with TOSS C3.

MOUNT AUBURN HOSPITAL

Tom Gallant,
IT Operations Manager
Mount Auburn Hospital

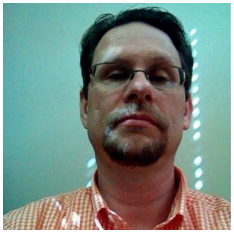
Responsive, Accurate, And Professional

The vBCDR ® project is a huge success. Implemented flawlessly and with no impact to our users, it was a very impressive accomplishment. TOSS C3's team is professional, responsive, and gets things done correctly. Ongoing support is excellent and I always get a quick and immediate response from TOSS C3. The hospital in now fully redundant on all IT levels and it is a great relief to management, our patients, and the entire IT staff.

Kim McMahon, Chief Operating Officer
Bove & Langa, P.C.

I Decided To Use TOSS C3 Because I Felt That They Were The Most Experienced And Had The Best Security

It is a load off my mind that our systems are constantly backed-up and I no longer have to manually do a daily back-up and physically store the media. Time and again TOSS C3 has had to recreate a master document that was written over, and they've always been able to retrieve it easily. TOSS C3 has also kept the firewalls and spam filters up to date while monitoring the servers 24/7, and they've supplied me with a written security plan. I feel that if anyone tried to hack us they would have a much more difficult time doing so against the TOSS C3 servers as opposed to an independent server located in our office space. I'm confident that TOSS C3 is doing everything possible to protect my firm.



Ed Bernard, Systems Administrator
Springfield Medical Care Systems

The Value Of What TOSS C3 Has Provided For Us More Than Compensates For Any Savings You Would Get From Any Comparable Organization

TOSS C3 has proved invaluable in monitoring, and in some cases restoring, our scheduled back ups, both locally and to the cloud. TOSS C3 has caught and prevented data loss on more than one occasion over the last seven years. The expertise and dedication TOSS C3 has provided to our company has been an asset time and time again in our Virtual, SAN, and SQL environment. We rely on TOSS C3 on a consistent basis to help us both maintain our environment and proactively prevent system failures, networking issues and software issues. I wholeheartedly recommend TOSS C3 for day-to-day consulting and short- and long-term planning for the IT needs of your business.

Michael Driscoll, President
Crosbie-MacDonald Insurance

Value Is The Key To Success

In my 25 years of buying computer services I learned that the value of TOSS C3 overshadowed the price. TOSS C3 was always there for me when things went wrong, but more importantly they prevented the problems before there was an issue. With the choice of various levels or service and pricing, you can pick the level that best suits your needs and in-house abilities. Having TOSS C3 monitor my system allowed me to focus on my business knowing that if there was a breach I had the secure backup of my data and a quick solution to the problem. The monitoring is also a key part of my disaster plan that every business must have in case their office suffers a physical loss that would prevent access to the server and equipment. Being able to set up off-site in a hurry is critical to client satisfaction.

O'Connor Carnathan and Mack LLC

Lynda Fitzpatrick, Legal Assistant
O'Connor, Carnathan & Mack, LLC

We Have Had Multiple IT Consultants Before TOSS C3 And None Did The Job As Well As Them

You do truly get what you pay for with IT consultants. There may be less expensive options, but when something goes wrong you will need someone capable of fixing the problem fast and correctly. TOSS C3 has been able to do that for us. When it comes to monitoring our network, we have left that in TOSS C3 control. We have had unexpected power outages in our office and TOSS C3 got us up and running with nothing lost. We also had a major scheduled power outage on a weekend and TOSS C3 had a representative here as we were coming in and made sure everything was up and running correctly.

Alan LaBatte, Chief Information Officer
UNO Restaurants, LLC

TOSS C3 Is Worth It Because Of The In-Depth Understanding They Have Of Our Company's Environment

If we have an issue that needs attention, we don't have to deal with a company that needs to be brought up to speed on our IT infrastructure. Knowing that backups, security and overall network health is being monitored is very important to us. If we relied totally on in-house resources we would not have the same level of confidence that we have appropriate coverage. Everyone would like to believe that they can do this all in-house, but doing so would lead to a less reliable environment. Other priorities can easily distract us from monitoring our network.

Dennis Honan, Director of Operations
Diocese of Manchester

Expertise, Savings and Great Customer Service. What More Could You Ask For?

TOSS has technology expertise far beyond our own capability, allowing us to deliver the most up-to-date solutions to our users at a fraction of the cost to do internally. TOSS is more responsive and cost effective than all others we have worked with. They provide a high degree of customer service, quickly resolve issues and they care! After talking with a few of their clients, I don't think there would be any doubt that TOSS is the best around!

O'Connor Carnathan and Mack LLC

William Hartzell, Paralegal
O'Connor, Carnathan & Mack, LLC

On Price, The Maxim Of 'You Get What You Pay For' Really Applies

In the course of our litigation work we have encountered many startup companies that tried to cut costs by using 'free' services like Google or Dropbox. While those services have a place, they are not the same as a robust, professional email and document handling system for a solid business platform. From my perspective, untangling these 'free' services has created more problems for these young companies as they mature. One company encountered significant data loss when they were acquired by a large corporation and attempted to port their data to their new corporate parent's system.

Susan Kuder, Director of Administration
Cunningham, Machanic, Cetlin, Johnson, Harney & Tenney, LLP

Immediate and Caring Response from Engineers Who Really Know What They Are Doing

We have been with TOSS for many, many years. They have provided consistent IT support. I can ask any question, and it will be answered. The immediate response to issues really separates TOSS from other services. TOSS is one of the first IT firms to go to Cloud Computing. They are reliable and knowledgeable. Their engineers will work with you until the problem is solved.

Michelle Woodbury, Owner
2Sisters Senior Living Advisors

I Save Time, Money and Frustration by Working with TOSS C3!

TOSS is very responsive. I can save time by not trying to figure out what my computer is doing, I call TOSS and you guys look into it right away! We have been so happy with the service and attention we get from TOSS!

Stu Kaffee, Owner
NL Fish & Company

As a Client of TOSS I'm Able to Focus on Running My Business, Not IT Issue!

By moving to the Cloud I have been able to concentrate on running my practice and not be concerned about any IT issues. I feel that the people at TOSS are responsive to our specific needs and understand the workings of our practice. I feel that TOSS is competitive with their pricing, but more importantly responsive when problems arise. The support group listens and then reacts to any problems.

Managing Corporate & Over 90 Remote Offices is a Breeze with TOSS!

Consistency. Having TOSS manage not only our corporate office IT needs but also our over 90 apartment complexes has made the managing of IT needs, issues, etc… a breeze. Availability and response time. TOSS is always ahead of the curve, proposing new and improved IT needs that are most cost effective for our firm and never trying to upsell. The availability of their Help desk as well as Sr. Engineers is one of the main reasons we have had a 20+ year relationship with TOSS.

Chris Pavoni,
Operations Manager
Hallkeen
Management

24/7 Support and Security of their Cloud Help Run My 3 Businesses!

The best thing about TOSS is the 24-7 support. I trust the security and backup of their Cloud. I have 3 locations and this has been a real asset. I find their ticket system works well.

Gretchen Fish,
Owner
GS Fish

Jeff Winer,
Owner
Jeff Winer CPA

Responsive Service with Personal Attention

The attentive personnel with the secure email service. Responsive. Not just email. Worked with us when server failed during tax season. Personal attention at all levels as required for the circumstances.

ANDERSON
KREIGER

Maria Machado,
Firm Administrator
Anderson & Kreiger LLP

Professional, Attentive and a Predictable Budget Make TOSS Our One-Stop IT Shop

The convenience and ease of working remote and a more predictable budget not having to worry about back end hardware. I like the one stop shop for all IT needs. Very professional and experienced engineers and very attentive to the firm's customized needs.

TOSS C3
153 Northboro Road, Bldg. 21
Southborough, MA 01772
(888) 966-9514
info@TOSSC3.com
www.TOSSc3.com

IT Services Provider Comparison Chart

23 Questions You MUST Ask Before Hiring An IT Support Company	Company A _____	Company B _____	Company C _____	TOSS C3 Cybersecurity | Cloud | Compliance
Do they answer their phones live?				✓
Do they have a written, guaranteed response time to support tickets you submit?				✓
Do they provide weekend and after-hours support, or is that extra?				✓
Do they take the time to explain things in plain English? No "geek speak"?				✓
Do their engineers arrive on time and dress professionally?				✓
Do they provide detailed invoices explaining what you are paying for?				✓
Do they have adequate cyber liability, errors and omissions, business liability and workers' comp insurance to protect YOU?				✓
Do they guarantee to complete projects on time and on budget IN WRITING?				✓
Do they insist on monitoring your network 24/7/365 to PREVENT problems from turning into downtime, viruses and other issues?				✓
Do they provide a regular report on backups, patches and updates so you know for sure that your systems are secure and protected?				✓
Do they provide you with full written network documentation?				✓
Do they have other technicians on staff who are familiar with your network, or are they a "one-man band" who could go sick or missing when you really need them?				✓
Is their "all-inclusive" support plan TRULY all-inclusive? What's NOT included?				✓
Do they insist on monitoring on-site AND off-site backups?				✓
Do they insist on doing periodic test restores of your backups?				✓
Do they insist on backing up your network BEFORE a project or upgrade?				✓
Will they provide a disaster recovery plan for getting your network restored fast in the event of a disaster as part of their service, or is that extra?				✓
Is their help desk US-based or outsourced overseas?				**Local And US Based!**
Do their technicians maintain certifications and participate in ongoing training?				✓
Do they provide cybersecurity training to your employees?				✓
Do they provide a comprehensive cybersecurity protection plan?				✓
Will they create and help you enforce an Acceptable Use Policy (AUP) for your staff?				✓
Will they take ownership of dealing with your ISP, phone company and line-of-business applications, or are you on your own?				✓
Your Clear Choice...				✓

LAYMAN'S GUIDE TO CYBERSECURITY, DATA COMPLIANCE, & CLOUD COMPUTING

Table of Contents

Introduction

TOSS C3'S LAYMAN'S GUIDE TO CYBERSECURITY, DATA COMPLIANCE, & CLOUD COMPUTING

Read this Free Guide and you'll discover:

- ✓ If your business is truly protected from Cybercrime
- ✓ The 7 most critical IT security protections every business must have in place NOW to protect themselves from cybercrime, data breaches, and hacker attacks.
- ✓ The 10 ways that hackers get around your firewall and anti-virus and rob you blind.
- ✓ How to make your employees care about cybersecurity.
- ✓ Top compliance concerns for the following industries: legal, healthcare/hospital, and public sector & education.
- ✓ The pros & cons of cloud computing.
- ✓ The different types of cloud solutions that are available and frequently asked questions.

Chapter One

Cybersecurity: Is Your Business Truly Protected?

Cybercrime is so widespread that it is practically inevitable that your business – large OR small – will be attacked. However, a few small preventative measures can prepare you and minimize (or outright eliminate) any reputational damages, losses, litigation, embarrassment and costs.

Unfortunately, when you fall victim to a cyber-attack, through no fault of your own, the first person that they will point the finger at is YOU. It's extremely unfair, isn't it**?** Victims of all other crimes – burglary, mugging, carjacking, theft – get sympathy from others. They are called "victims," and assistance and support come flooding in. But if your business is the victim of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will instantly be labeled as stupid or irresponsible.

Additionally, you will be investigated and questioned about what you did to prevent this from happening. If the answer is not adequate, you can be found liable, facing serious fines and lawsuits. You will be required by law to tell your clients and/or patients that YOU exposed their private records, financials and data to a criminal. Your competition will have a heyday over this, and clients will leave in droves once they discover that you have been compromised. Your bank will NOT come to your rescue either, and unless you have a very specific type of crime insurance, **any financial losses will not be covered**.

Here's the Ugly Truth:

You already know that cybercrime is a very real threat to you – but it's very possible that you're underestimating the potential damage, OR that **you are being ill-advised** and underserved by the employees and/or vendors that you hired to protect your business from these threats.

ONE cyber-attack…one slipup from even a smart, tenured employee clicking on the wrong e-mail…can open the door to ABSOLUTE FINANCIAL DEVASTATION, and undo everything that you've worked so hard to achieve. **Take the story of Michael Daugherty, former CEO of LabMD.** His $4 million Atlanta-based company tested blood, urine, and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA.

He HAD an IT team in place that he **believed** was protecting the company from a data breach – yet the manager of his billing department was able to download a file-sharing program to the company's network to listen to music, and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network. This allowed an unscrupulous IT services company to hack in and gain access to the file and use it against them for extortion. When Daugherty refused to pay them for their "services," the company reported him to the Federal Trade Commission, who then came knocking. After filing some 5,000 pages of documents to Washington, he was told the information he had shared on the situation was "inadequate," and the FTC requested in-person testimony from the staff regarding the breach, and more details on what training manuals he had provided to his employees regarding cybersecurity, documentation on firewalls, and penetration testing. (Question: Are you doing any of this now?)

Long story short, his employees blamed HIM and left. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies. The emotional strain on him – not to mention the financial burden of having to pay attorneys – took its toll, and eventually he closed the doors to his business, jamming medical equipment into his garage where it remains today (image below).

Bloomberg

A Leak Wounded This Company. Fighting the Feds Finished It Off

Michael Daugherty learns the high price of resistance.

By Dune Lawrence | April 25, 2016

Photographs by Johnathon Kelso for Bloomberg Businessweek

From **Bloomberg Businessweek**

Right now, you're thinking "Not my company…not my people…"

Currently, you do not believe that you are in danger because you're "small" and not a big target like J.P. Morgan or Home Depot. You have "good" people and protections in place. Time to think again. Every single day, 978,000 NEW malware threats are being released, and MORE than HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about them because it's kept quiet for fear of attracting bad PR, lawsuits, and data-breach fines. Make no mistake: small businesses are being compromised daily, and the smug ignorance of "that won't happen to me" is an absolute surefire way to leave yourself wide open to these attacks.

In fact, the National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year**. That number is growing rapidly as more businesses utilize cloud computing and mobile devices, storing more information online.

You can't turn on the TV or read a newspaper without learning about the latest online data breach. Government fines and regulatory agencies are growing in number and severity. Because of all of this, it is critical that you have security measures in place. In the following chapters, we will discuss security protections that you should have in place, how hackers get around your firewall and rob you blind, and how to get your employees to care about cybersecurity.

Chapter Two

7 Critical Security Protections Every Business Must Have

Many business owners are shocked when they get compromised because they BELIEVED that their IT company or guy had it "handled." However, there is a virtual army of thousands of hackers and very sophisticated crime rings that work around the clock to overcome known protections – and you can't stop a brand-new threat that was invented yesterday with a security system that was designed six months to a year ago. It requires special expertise to stay on top of all of this, which is why many don't.

Below, are the seven security protections that your business should have in place to protect the company from cybercrime, data breaches, and hacker attacks. Ask yourself, is your company actually implementing ALL of these protocols –OR if you don't know if you are – WHY NOT? What hasn't your current IT company told you about all of this?

1. **The #1 Security Threat to ANY Business Is**...YOU! Like it or not, almost all security breaches in business are due to an employee clicking, downloading, or opening a file that's infected, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all of the other PCs on the network. Phishing e-mails (an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor that you trust) are still a very common occurrence. Unfortunately, spam filtering and antivirus alone cannot protect your network if an employee is clicking on and downloading the virus. That's why it is CRITICAL that you educate all of your employees in how to spot an infected e-mail or online scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is ONE SLIPUP. Because of this, it is critical that employees are constantly reminded and educated regarding cybersecurity threats and best practices.

2. On that same theme, the next precaution is implementing an Acceptable Use Policy. An AUP outlines how employees are

permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employee's access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

Having this type of policy is particularly important if your employees are using their own personal devices and home computers to access company e-mail and data. With so many applications in the cloud, an employee can access a critical app from any device with a browser, which exposes you considerably.

If an employee is logging in to critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter YOUR network – which is why we don't recommend you allow employees to work remote or from home via their own personal devices.

Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it is a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

3. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator, so employees are not able to get lazy and choose easy-to-guess passwords, putting your organization at risk. Are they? If you and your employees are not being forced to do a password reset every 30-60 days, you are putting company data and information at risk.

4. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in common software programs that you are using, such as Adobe, Flash, Microsoft or QuickTime; therefore, it is critical that you patch and update your systems and applications when patches become available. If you are under a managed IT plan, this can all be automated for you so you do not need to worry about an employee missing an important update.

5. **Have A Business-Class Image Backup BOTH On-Premise and In The Cloud.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you will not need to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, and against natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

6. **Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department.** The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all that it takes is a known username and password. Employees are now asking if they

can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

While this trend can be convenient, it has DRASTICALLY increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); the biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application.

So if you ARE going to let employees use personal devices and home PCs, you need to make sure that those devices are properly secured, monitored and maintained by a security professional. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

But here is the major issue: most employees will not want you monitoring and policing their personal devices; nor will they like that you will wipe their device of all files if it's lost or stolen, however, that is exactly what you will need to do to protect your company. Our suggestion is that you allow employees to access work-related files, cloud applications and e-mail only via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi.

7. **A Business-Class Good Firewall and Proper Updates.** A firewall acts as the frontline defense against hackers blocking everything that you have not specifically allowed to enter (or leave) your computer network. To be effective, all firewalls need monitoring and maintenance, just like all devices on your network, or they are completely useless. This should also be performed by your IT person or company as a part of their regular, routine maintenance. HOWEVER, it is not uncommon for an IT guy to

forget to turn on one or more of the intrusion detection and prevention features; often they are disabled to work on the firewall, but then never turned back on, rendering the device useless.

8. **Protect Your Bank Account.** Did you know that your company's bank account does not enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many people think that FDIC protects you from fraud; it does NOT. It protects you from bank insolvency, NOT fraud.

   So here are three things that you can do to protect your bank account. First, set up e-mail alerts on your account so that you are notified any time money is withdrawn. The FASTER that you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY that it happens can be stopped. If you discover it even 24 hours later, you may be out of luck. That is why it's critical that you monitor it daily and contact the bank IMMEDIATELY if you see any suspicious activity.

   Second, if you do online banking, dedicate ONE computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc., with that PC. Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date antivirus software.

   Finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards that are associated with that account. Taking all of these measures will greatly improve the security of your accounts.

Are you really willing to be complacent about this?

Look, I know that all of this appears to be a giant distraction and cost that interferes with REAL work. You and I both realize that implementing proper security protocols won't win you the "employer of the year" award or deliver an ROI – in fact, we HOPE that by doing OUR job, it never has to deliver one.

However, if you foolishly choose to turn a blind eye and be arrogant, complacent or careless, cybercriminals WILL take advantage of you. You WILL pay the ransom…NOT your failing IT company that was SUPPOSED TO PROTECT YOU. This tsunami of pain will land directly on YOUR desk to deal with, everyone pointing the blame at YOU. YOUR bank account. YOUR business. You will be faced with significant losses, costs and an emotional drain on you and your team as you deal with a breach.

Mark Twain once said, "Supposing is good, but knowing is better"

If you want to know for SURE that your current IT company (or IT person) is truly doing everything that they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a FREE Security and Backup Audit.

At no cost or obligation, we'll conduct a free Security and Backup Audit of your company's overall network health to review and validate as many as 27 different data-loss and security loopholes, including small-print weasel clauses used by all third-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose – and (more importantly) how FAST could you get your IT systems back online if hit with ransomware? We'll reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent? Are they downloading illegal files (music and video) and exposing you, as happened with LabMD?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently, and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines if a breach happens and the investigation reveals YOU didn't take necessary precautions – and ignorance is not an acceptable excuse that will get you out of a lawsuit.

- Is your firewall and antivirus configured properly and up-to-date? No security device is "set and forget." It needs to be constantly monitored and updated – is yours? Is your IT company giving you the assurances that it is?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup? Could they walk off the job with a list of all your clients and go work for a competitor?

I know that it's natural to want to think, "We've got it covered." **Yet I can practically guarantee that my team will find one or more ways**

that your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the thousands of businesses that we've audited over the years.

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a third party to validate that nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

Chapter Three

How Hackers Get Around Your Firewall and Anti-Virus

With cybercrime at an all-time high, hackers are setting their sights on small and medium businesses who are "low hanging fruit." Do not be their next victim! Wondering how hackers get around the firewalls and anti-virus programs to rob you blind? This chapter reveals the most common ways that hackers get into your network and how you can protect your company today.

1. **They Take Advantage of Poorly Trained Employees.** The #1 vulnerability for business networks are the employees that are using them. It is extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (an e-mail that is cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **They Exploit Device Usage Outside of Company Business.** You must maintain an Acceptable Use Policy that outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your employee's access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

   Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data. If an employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos,

texts, etc. ensuring that YOUR clients' information isn't compromised? These are all important points to consider when creating and maintain an Acceptable Use Policy.

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

3. **They Take Advantage of WEAK Password Policies.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

4. **They Attack Networks That Are Not Properly Patched with The Latest Security Updates.** New vulnerabilities are frequently found in common software programs that you are using, such as Microsoft Office; therefore, it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you do not need to worry about missing an important update.

5. **They Attack Networks with No Backups or Simple Single Location Backups.** Simply having a solid, reliable backup can foil some of the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also provide protection against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

6. **They Exploit Networks with Employee Installed Software.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. This can largely be prevented with a good firewall and employee training and monitoring.

7. **They Attack Inadequate Firewalls.** A firewall acts as the frontline of defense against hackers, blocking everything that you haven't specifically allowed to enter (or leave) your computer network. To be effective, all firewalls need monitoring and maintenance, just like all of the devices on your network. This should also be done by your IT person or company as a part of their regular, routine maintenance.

8. **They Attack Your Devices When You're Off of the Office Network.** It's not uncommon for hackers to set up fake clones of public WiFi access points to try and get you to connect to THEIR WiFi over the legitimate, safe public one that is being made available to you. Before connecting, check with an employee of the store or location to verify the name of the WiFi that they are providing. Next, NEVER access financial, medical or other sensitive data while on public WiFi. Also, don't shop online and enter your credit card information unless you're absolutely certain that the connection point that you're on is safe and secure.

9. **They Use Phishing E-mails to Fool You Into Thinking That You're Visiting A Legitimate Web Site.** A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site that you trust in an effort to get you to willingly enter your login information to a particular web site or to click and download a virus.

   Often, these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That is what makes these so dangerous – they LOOK exactly like a legitimate e-mail.

10. **They Use Social Engineering and Pretend To Be You.** This is a basic 21st-century tactic. Hackers pretend to be you to reset your passwords. In 2009, social engineers posed as Coca-Cola's CEO, persuading an exec to open an e-mail with software that infiltrated the network. In another scenario, hackers pretended to be a popular online blogger and got Apple to reset the author's iCloud password.

Do you want help, ensuring that your company has all ten of these vulnerabilities covered?

If you're concerned about employees and the dangers of cybercriminals gaining access to your network, contact us. We would be happy to discuss how we can implement a managed security plan for your business.

At no cost or obligation, we would be happy to conduct a Security Assessment which will assess the company's overall network health to review and validate as many as 27 different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL of the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.

- Is your firewall and antivirus configured properly and up-to-date?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

It is natural to think, "We've got it covered," however, I can practically guarantee that my team will find one or more ways that your business is at serious risk for hacker attacks, data loss, and extended downtime – I've seen it too often in all of the thousands of businesses that we have audited over the years.

Even if you have a trusted IT person or company who put your network in place, it never hurts to have a 3rd party to validate that nothing was overlooked. We have no one to protect and no reason to conceal or gloss over anything that we find. If you want the straight truth, we will report it to you.

You have spent a lifetime working to get where you are. No one gave you anything. You earned every penny and every client. Why would you risk losing it all? Get the facts and be certain that your business, your reputation, and your data are protected.

Chapter Four

How to Make Your Employees Care About Cybersecurity

While employees are a company's greatest asset, they are also a company's greatest security risk. Updating employees on an annual basis, regarding best security practices, is not enough. Instead, employee training should be treated similar to updating hardware or operating systems. Employees should be consistently updated on the latest security vulnerabilities and trained on how to recognize and avoid them. Below, are 8 tips on how to train employees to understand cyber risk and best practices.

1. **Conduct "Live Fire" Training Exercises.** Using your security department, or an outside vendor, simulate an attack that would be related to their job. For example, a fake phishing email could be sent to employees across the organization and the number of clicks tracked. From there, the data can be broken down by department and types of message, allowing future training to be tailored to specific problem areas.

2. **Promote Cyber Awareness From Day One.** During the employee onboarding process, include cyber security training. Building a mindset of security awareness during the onboarding process will allow employees to understand that not only is it important, but that they will be receiving continuous updates and training on the topic, as threats change.

3. **Conduct Evaluations.** Performing periodic evaluations of employees and systems allow you to determine how vulnerable your organization is to attack. These evaluations also allow you to determine where improvements and further training are needed.

4. **Communicate.** In order to have all employees on the same page, create a plan for how to best communicate cybersecurity information to everyone. Get all departments on board with training and learning best practices – creating alignment throughout the company.

5. **Create a Formal Plan.** IT members should create a formal, documented plan for cybersecurity training. This plan should be regularly reviewed and updated with the latest information on attack vectors and other risks.

6. **Offer Continuous Training.** As attack vectors and other risks change frequently, cybersecurity training should occur throughout the year, at all levels of the organization, specific to each employee's department/job.

7. **Stress the Importance of Security at Work and at Home.** Teaching employees that the privacy and security lessons learned at work, also apply at home and in their personal lives, is important because it promotes continuous awareness.

8. **Reward Employees.** Reward employees who find malicious emails and discuss stories of those who helped thwart security issues. When mistakes are made, IT leaders should also empathize with those employees. Even with the best training and advice, mistakes will happen.

While training and educating your employees can help prevent attacks, there are still a small percentage of attacks that will get through. For this reason, it is important to have a solid, reliable IT team on your side, ensuring that your company's data and information is secure.

Chapter Five

Compliance Concerns

For highly regulated industries – legal, financial, healthcare – compliance is a major consideration when making the transition to cloud computing. There are a number of laws and regulations, such as Gramm-Leach-Bliley, Sarbanes-Oxley, and HIPAA, that require companies to control and protect their data and certify that they have knowledge and control over who can access this data, who sees it and how, and where it is stored. In a public cloud environment, this can be an issue. In fact, Office 365 and Google truly have no knowledge of where your data is, physically.

Most cloud providers have certifications which require them to be able to describe exactly what is happening in their environment, how and where the data comes in, what the provider does with it, and what controls are in place over the access to and processing of the data. As the business owner, it is YOUR neck on the line if the data is compromised, so it is very important that you ask them for validation that they are meeting the various compliance regulations on an ongoing basis. In this chapter, we break down the top compliance concerns by industry.

Legal Industry

Law firms are built on reputation management. Because of this, it is especially important that firms adapt their technology to protect their data. Law firms are attractive cyber-attack targets because they not only hold valuable client information, but they are regularly emailing attachments to clients, providing a possible means to enter client systems. Additionally, with hackers increasingly turning to ransomware to profit off of stolen data, law firms are particularly attractive targets due to the vast amount of confidential client data that they hold. Cybersecurity should be of utmost importance to firms as they can face hidden consequences as a result of a data breach such as increased insurance premiums, loss of intellectual property, and lost contract revenue.

As third parties, law firms are considered risks and clients for law firms are third-party risks. Because firms are classified as third-party vendors, they are required to have written cybersecurity plans, in addition to annual risk-assessments, and report cyber events when they happen. Annual risk-assessments should include overall security and penetration testing, in addition to external tests that determine what part of the system is at risk on the internet, testing vulnerabilities in web and mobile applications, and testing the security of wireless technology. Understanding the results of this assessment is especially valuable as it allows your defenses and cybersecurity plan to be designed accordingly.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is an EU-wide data protection law that supersedes previous national privacy laws. While the GDPR is a European regulation, US law firms need to be aware of whether they are in compliance, particularly when working with offices, cases, witnesses or clients in jurisdictions where the GDPR is enforced. Firms should assess whether their procedures for transferring, maintaining, protecting, and disposing of third party data comply with the new rules. Additionally, it is critical that firms evaluate and question whether their associated service providers and vendors, with access to client information, have the safeguards in place. Firms cannot afford to assume that these third parties already have the appropriate compliance measures in place.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA law requires that any organization that creates, receives, maintains or transmits PHI (protected health information) needs to conduct a thorough HIPAA risk assessment, in order to comply with §164.308 of the HIPAA Security Rule. This directly applies to law firms that deal with PHI. In December 2014, the Office for Civil Rights (OCR) revealed that 40% of all HIPAA breaches of more than 500 patients were attributed to negligent business associates (a category that includes law firms).

To avoid major fines, a HIPAA Risk Assessment should be conducted to identify potential risks and vulnerabilities to the confidentiality, availability, and integrity of all PHI that an organization creates, receives, maintains, or transmits. Guidelines to meet these objectives are as follows:

- Identify where PHI is stored, maintained, or transmitted.
- Identify and document potential threats and vulnerabilities.
- Assess current security measures used to safeguard PHI.
- Assess whether the current security measures are used properly.
- Determine the likelihood of a "reasonably anticipated" threat.
- Determine the potential impact of a breach of PHI.
- Assign risk levels for vulnerability and impact combinations.
- Document the assessment and take action where necessary.

Note that a HIPAA Risk Assessment is not a one-time exercise and should be reviewed periodically and as new work practices are implemented and introduced.

Healthcare Industry

The healthcare industry is a continual target for cyberattacks due to the vast amount of electronic data that flows through the medical community every day. Threats like ransomware, employee negligence, a growing demand for medical records in the black market, and device-dependent healthcare lacking adequate security pose large vulnerabilities for the healthcare industry, if they are not addressed. With these factors in mind, healthcare data security must be a top priority. Now is a critical time for healthcare providers to invest in experts who can help them with their cybersecurity needs. Below is a list of the top compliance concerns for the healthcare industry.

Health Insurance Portability and Accountability Act (HIPAA)

The Department of Health and Human Services and the Office for Civil Rights (OCR) oversee the HIPAA Privacy and Security Rules. They

are responsible for investigating healthcare providers and their business associates to ensure that patient information remains protected.

HIPAA law requires that any organization that creates, receives, maintains or transmits PHI (protected health information) needs to conduct a thorough HIPAA risk assessment, in order to comply with §164.308 of the HIPAA Security Rule.

Although there is no specific risk analysis methodology, the US Department of Health and Human Services (HHS) recommends that an organization should follow these guidelines in conducting their risk assessment:

- Identify where PHI is stored, received, maintained or transmitted.
- Identify and document potential threats and vulnerabilities.
- Assess current security measures used to safeguard PHI.
- Assess whether the current security measures are used properly.
- Determine the likelihood of a "reasonably anticipated" threat.
- Determine the potential impact of a breach of PHI.
- Assign risk levels for vulnerability and impact combinations.
- Document the assessment and take action where necessary.

Note that a HIPAA Risk Assessment is not a one-time exercise and should be reviewed periodically and as new work practices are implemented and introduced.

Health Care Compliance Program and HIPAA Requirements

The following is a list of the compliance requirements of HIPAA:

- Conducting internal monitoring and auditing
- Implementing policies and written standards of conduct
- Designating a compliance officer and committee
- Conducting effective training and education
- Developing effective lines of communication
- Conducting internal monitoring and auditing
- Enforcing standards through well-publicized disciplinary guidelines
- Responding promptly to detected threats

In addition to these requirements, it is recommended that the following areas be addressed in a compliance plan, as it will adherence to the mandated areas more manageable.

- Evaluation of compliance risk areas
- Hiring practices
- Healthcare insurance and billing compliance
- Medical records releases and informed consents
- Medical necessity and documentation
- Business and medical records and retention
- Confidentiality
- Patient rights
- Employee safety, rights and obligations, and environmental concerns

Mobile and Digital Health Tools

According to the 8th Annual Industry Pulse Report from Change Healthcare and the Healthcare Executive Group, healthcare data privacy and security concerns are pushing healthcare payers and providers to reconsider whether they want to adopt mobile and digital health tools. This has prevented mobile and digital health tools from being widely adopted throughout the medical field, as the threat of PHI being compromised, is a major concern.

Public Sector & Education

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is an EU-wide data protection law that supersedes previous national privacy laws. While the GDPR is a European regulation, the US Public Sector and Educational Institutions also need to be aware of whether they are in compliance. The application of GDPR to the processing of personal information by public authorities is context dependent, and public sector customers will need to individually assess the applicability of GDPR to their activities. To avoid potential GDPR compliance issues, it is critical that both legal and technological teams are consulted.

Chapter Six

What is Cloud Computing?

Wikipedia defines cloud computing as, "The use and access of multiple server-based computational resources via a digital network (WAN, Internet connection using the World Wide Web, etc.)."

But what does *that* mean?

The easiest way to not only understand what cloud computing is but also gain insight into why it's gaining in popularity, is to compare it to the evolution of public utilities. For example, let's look at the evolution of electricity.

Back in the industrial age, factories had to produce their own power in order to run machines that produced the hard goods they manufactured. Be it textiles or railroad spikes, using machines gave these companies enormous competitive advantages by producing more goods with fewer workers and in less time. For many years, the production of power was every bit as important to their company's success as the skill of their workers and quality of their products.

Unfortunately, this put factories into TWO businesses: the business of producing their goods and the business of producing power. Then the concept of delivering power (electricity) as a utility was introduced by Thomas Edison when he developed a commercial-grade replacement for gas lighting and heating using centrally generated and distributed electricity. From there, as they say, the rest is history.

The concept of electric current being generated in central power plants and delivered to factories as a utility caught on quickly. This meant manufacturers no longer had to be in the business of producing their own power. **In fact, in a very short period of time, it became a competitive necessity for factories to take advantage of the lower cost option being offered by public utilities**. Almost overnight, thousands of steam engines and electric generators were rendered obsolete and left to rust next to the factories they used to power.

What made this possible was a series of inventions and scientific breakthroughs – but what drove the demand was pure economics. Utility

companies were able to leverage economies of scale that single manufacturing plants simply couldn't match in output or in price. In fact, the price of power dropped so significantly that it quickly became affordable for not only factories but every single household in the country.

Today, we are in a similar transformation following a similar course. The only difference is that instead of cheap and plentiful electricity, advancements in technology and Internet connectivity are driving down the costs of computing power. With cloud computing, businesses can pay for "computing power" like a utility without having the exorbitant costs of installing, hosting, maintaining, upgrading, and supporting it.

In fact, you are probably already experiencing the benefits of cloud computing in some way but hadn't realized it. Below are a number of cloud computing applications, also called SaaS or "software as a service," you might be using:

- Facebook, Gmail, Hotmail or other free e-mail accounts
- NetSuite, Salesforce
- Constant Contact and other e-mail broadcasting services
- Zoomerang, SurveyMonkey and other survey tools
- LinkedIn
- Twitter
- All things Google (search, AdWords, maps, etc.)
- iCloud, DropBox, EverNote and other storage services

If you think about it, almost every single application you use today can be (or already is) being put "in the cloud" where you can access it and pay for it via your browser for a monthly fee or utility pricing. You don't purchase and install software but instead access it via an Internet browser.

What About Office 365 and Google Apps?

Office 365 and Google Apps are perfect examples of the cloud computing trend. For an inexpensive monthly fee, you can get full access and use of Office applications that used to cost a few hundred dollars or more to purchase. Additionally, since these apps are being powered by the cloud provider, you don't need an expensive desktop with lots of power to use them – just a simple Internet connection will do on a laptop, desktop, tablet, or mobile device.

Of course, these aren't great options for all businesses. Google Apps doesn't integrate with many line-of-business applications, which presents a deal breaker for using this service. For example, if you like using Microsoft's Excel or Word to pull reports or create documents from your line of business application, you might not be able to do that with Google Apps. Gmail, Google's answer to Microsoft's Exchange server and Outlook combination, is very free-form and open. Many of our clients who have tried Gmail quickly become frustrated and request to return to Outlook.

Microsoft's Office 365 is a great platform for some companies and due to key limitations, make it a poor choice for many businesses, not to mention that customers get near-zero help desk support. The limitations pop-up quickly once you need to implement a non-Microsoft technology with your "servers" in the Office 365 Cloud. For example, if you have a line of business application such as QuickBooks or Autonomy which require fast access to your servers, Microsoft is not going to install a dedicated custom system for you or anyone else, since it does not fit their "cookie cutter model." If something goes wrong, there isn't a customer service help desk that offers immediate support or assistance. But again, it's a perfect example of where the industry is headed to anticipate the needs for cloud computing.

Here's an interesting set of questions to ponder while considering these or any cloud based solution:

- Where will my data reside?
- How many copies of my data will be out in the cloud?

- Who will have physical access to my data?
- Who is responsible for backing up my data and how will I recover it when necessary?
- If I decide to switch providers, how will my data be properly destroyed along with all copies, and what guarantee will I have that my data was properly destroyed?

Chapter Seven

Pros & Cons of Moving to the Cloud

As you read this section, keep in mind that there is no "perfect" solution. All options – be it an in-house network or a cloud solution – have both upsides and downsides. Your selection has to be determined on a case-by-case scenario before you can come to a complete conclusion on which option will work best for you. (Warning: Do not let a cloud expert tell you that there is only "one way" of doing something.) Some companies end up with a **hybrid solution** where some of their applications are in the cloud and some are still hosted and maintained from an in-house system.3 We'll discuss more of this in a later section. Here are the general pros and cons of cloud computing:

Pros of Cloud Computing

- **Lowered IT costs.** This is probably the single most compelling reason why companies choose to move their network (all or in part) to the cloud. You'll save money on software licenses, hardware (servers, laptops, and workstations) as well as on IT support and upgrades. In fact, we save our clients an average of 20% to 50% when we move some or all of their network functionality to the cloud. **So if you hate constantly writing big, fat checks for IT upgrades, you will really want to look into cloud computing.**

- **Ability to access your desktop and/or applications from anywhere on any device.** If you travel a lot, have remote workers or prefer to use an iPad while traveling, a laptop at your house, and a PC from the office, then cloud computing will give you the ability to work from any of these devices. This benefit of work any time, from anywhere, on any device, consistently ranks as a top 3 benefit from all client and market surveys TOSS C^3 conducts.

- **Disaster recovery and backup are automated.** The servers in your office are extremely vulnerable to a number of threats including viruses, human error, hardware failure, software corruption, power outage, and, of course, physical damage due to a fire, flood or other natural disaster. If your servers were in the cloud and your office was reduced to a pile of rubble, you could purchase a new laptop and be back up and running immediately. This would NOT be the case if you had a traditional in-house network and were using tape drives, CDs, USB drives, online backup services, or standard disk to disk devices to back up your system.

  Synonymous to a public utility, cloud platforms are far more robust and secure than your average business network, because they utilize economies of scale to invest heavily into security, redundancy, and failover systems making them far less likely to go down. This in itself is a budget saver. The dollars being spent now on backup services, tapes, and the cost of downtime when a recovery is required, are all returned back to the bottom-line.

- **It's faster, cheaper, and easier to set up new employees.** If you have a seasonal workforce or a lot of turnover, cloud computing will not only lower your costs of setting up new accounts, but it will make it infinitely faster. *"TOSS C³ currently provides cloud IT for a local firm that brings on an average of 10 extra summer interns in May through August. If they had a traditional network setup, they would have to purchase expensive PCs and software licenses for these temporary workers and then pay to maintain and upgrade them throughout the year. Using cloud computing, these interns use their own laptops and log into the network securely. The firm ONLY pays for those workers' licenses during the time when they are interning, just like a utility. When September comes around, they no longer pay for those licenses and support. Using this model saves them approximately $27,000 a year in hardware, software and IT services."*

- **You use it without having to "own" it.** More specifically, you don't own the *responsibility* of having to install, update, and maintain the infrastructure. Think of it similar to living in a

condo where someone else takes care of the building maintenance, repairing the roof, and mowing the lawn, but you still have the only key to your section of the building and use of all the facilities. This is particularly attractive for companies who are new, expanding, or facing a major IT upgrade, and don't want the heavy outlay of cash for purchasing and supporting an expensive computer network. Simply put, IT as a Utility®, takes the variable Capital (CAPEX), Operating (OPEX), and Human Resource expenses you are pouring into IT, off of your income statement and balance sheet and replaces them with a predictable and scalable single line-item under your monthly utility (IT) expenses.

- **It's a "greener" technology that will save on power and your electric bill.** For some smaller companies, the power savings will be too small to measure. However, for larger companies with multiple servers who are cooling a hot server room and keeping their servers running 24/7/365, the savings are considerable. *One of our clients had 4 cabinets of servers and storage costing them $4,700.00 on average per month for power and cooling, which was eliminated when they moved to the cloud.*

- **It's an "offsite" system that will save on real-estate costs.** Real-estate is expensive and with the economy turning around, the cost per square foot won't be coming down any time soon. Smaller companies can reclaim the server room and put it to better use while larger companies can reclaim large areas or an entire floor, not to mention the expensive rent being spent on co-location facilities and other redundant offsite locations and data centers.

Cons of Cloud Computing

- **The Internet going down.** While you can mitigate this risk by using a commercial grade Internet connection and maintaining a secondary backup connection, there is a chance that you will lose Internet connectivity, making it difficult to work from the office.

- **Data security.** Many people don't feel comfortable having their data in some offsite location. This is a valid concern and before you choose any cloud provider, you need to find out more information about where they are storing your data, how it's encrypted, who has access to it, and how you can get it back.

- **Certain line-of-business applications won't work in the cloud**. For example, AutoCAD and 3D-rendering, some lab equipment and manufacturing systems that need a rapid high-speed interface between software and machinery. In Google or Office 365's cloud, in fact, no line of business application will work that is not part of their cloud offering.

- **Compliance Issues.** As was discussed in Chapter Five, most cloud providers have certifications which require them to be able to describe exactly what is happening in their environment, how and where the data comes in, what the provider does with it, and what controls are in place over the access to and processing of the data. As the business owner, it's YOUR neck on the line if the data is compromised, so it's very important that you ask for some type of validation that they are meeting the various compliance regulations on an ongoing basis.

  Some key questions that you will want to know the answers to are: Where is the data located? Who has access to it? How is the data being stored in production and in DR? Is the data encrypted in-flight and at rest?

- **Intimate knowledge of your system for support.** When everything's working, the cloud is great. What happens when you can't access an application or your data? 24/7/365 support from knowledgeable engineers who know your company and your system is crucial. Nothing can be more frustrating than getting an overseas level-1 support tech who's reading from a prompter, following a generic script, and wasting your time and money.

Chapter Eight

Different Types of Cloud Solutions & FAQs

As was previously stated, there is no "perfect" solution when making the transition to cloud computing. Your selection has to be determined on a case-by-case scenario before you can come to a complete conclusion on which option will work best for you and your company. The descriptions below give you a better idea of what the different types of cloud solutions entail.

Pure Cloud: This is where all your applications and data are put on the other side of the firewall (in the cloud) and accessed through various devices (laptops, desktops, iPads, and mobile devices) via the Internet.

Hybrid Cloud: Although "pure" cloud computing has valid applications, for some, it can be a scary first step. A hybrid cloud enables you to put certain pieces of your existing IT infrastructure (say, Business Continuance and Disaster Recovery) in the cloud, while the remainder of the IT infrastructure stays on premise. This gives you the ability to enjoy the costs savings and benefits of cloud computing where it makes the most sense without the risk of being out of compliance, if you are in a highly regulated industry.

Point Solutions: Another option would be simply to put certain applications, like Microsoft Exchange, Email Encryption, CRM, or Accounting in the cloud while keeping everything else onsite. Since e-mail is usually a critical application that everyone needs and wants access to on the road and on various devices (iPad, smart phone, etc.) then often this is a great way to get advanced features of Microsoft Exchange without the cost of installing and supporting your own in-house Exchange Server, Operating System, and Licensing.

Public Cloud vs. Private Cloud: Public Clouds are services that anyone can tap into with a network connection and a credit card. They are shared infrastructures that allow you to pay-as-you-go and managed through a self-service web portal. Private clouds are essentially custom built infrastructures that mimic public cloud services, but are on premise. Private clouds are often the choice of companies who want the

benefits of cloud computing, but don't want their data held in a public or offsite environment. Another term used today for Private Clouds is Converged Infrastructure. If you are in a highly regulated industry, then a private or a hybrid cloud makes sense.

Cloud Computing FAQs About Security, Where Your Data Is Held, and Internet Connectivity

Question: What if my Internet connection goes down for an extended period of time?

Our Answer: While this is a valid concern, TOSS C^3 offers a service called WAN-UP™ which takes two or more wired and or wireless internet services from different providers and connects them to the supplied 24/7 managed appliance. Once connected, the appliance will aggregate the bandwidth giving you full usage of all bandwidth purchased. In the event of an internet line failure, the appliance automatically routes your access to another available line. The result is super-fast access when all lines are up and not losing access if one internet line goes down. You can connect from 2 to 26 separate internet lines with WAN-UP™.

Question: What happens if we lose power or can't get to the office, how can we continue to work productively?

Our Answer: One of the many problems our IT as a Utility® cloud offering solves, is continuous access from any device and from any location. Since your IT infrastructure is liberated from your office, power outages, building shutdowns, storms, and other mishaps have zero impact on your IT system. This allows you and your staff to use any device that can get an internet connection and securely login into your IT as a Utility® system enabling you to conduct business as usual with no diminishment of service.

Question: What about security? Isn't there a big risk of someone accessing my data if it's in the cloud?

Our Answer: In many cases, cloud computing is a MORE secure way of accessing and storing data. Just because your server is onsite doesn't make it more secure. In fact, most businesses can't justify the cost of securing their network the way a cloud provider can. Most security breaches occur due to human error; one of your employees downloads a file that contains a virus, they don't use secure passwords, or they simply e-mail confidential information out to people who shouldn't see it. Other security breaches occur in on-site networks because the company didn't properly maintain their own in-house network with security updates, software patches, and up-to-date anti-virus, and firewalls. That's a FAR more common way networks get compromised verses a cloud provider getting hacked. At TOSS C^3, we use clusters of highly available firewalls, intrusion detection systems, and 2-factor authentication is available as an option. Additionally, all data at the production and Disaster Recovery facilities is encrypted both at rest and in-flight.

Question: Can someone tap into my cloud connection and read my email or get my data?

Our Answer: Most providers have some form of encryption for your cloud connection that prevents this from happening. Your connection to TOSS C^3's IT as a Utility® completely mitigates this by keeping all of the data, applications, and processing securely in the cloud data centers so your connection has no information within it other than video signaling, sound, keyboard strokes, and mouse movements. When you do download or print a file, the data is encrypted prior to sending it to you and the entire time it takes to get to your device, so security is not an issue.

Question: What if we don't like the cloud? How do I get my data back?

Our Answer: We give every client detailed information that clearly outlines where their data is and how they could get it back in the event of an emergency. This includes emergency contact numbers, information on how to access your data and infrastructure without

needing our assistance (although we are always available to support you,) and information regarding your backups and licensing.

In fact, you should never hire ANY IT professional that won't give you that information. We also have the ability, with our vBCDR® system, to replicate your data every day to your office so you have a physical copy and back up of your entire network to guarantee that your applications, servers, and data are always accessible by you. vBCDR®, which stands for Virtual Business Continuity and Disaster Recovery, is a patent pending system TOSS C^3 developed in conjunction with DELL and utilizes TOSS' Cloud on Write™ technology. vBCDR® is an invaluable and robust optional service protecting files, folders, applications, servers, sites, and the enterprise.

Question: Do I have to purchase new hardware (servers, workstations) to move to the cloud?

Our Answer: No! That is one of the best benefits of cloud computing. It allows you to use older workstations, laptops and servers because the computing power is in the cloud. Not only does that allow you to keep and use hardware longer, but it allows you to buy cheaper workstations and laptops because you don't need the expensive computing power required in the past. Ninety-nine percent of our clients use their existing equipment or low-cost laptops, and those who add additional systems, usually purchase cloud terminals, which are very low-cost purpose built appliances that boot directly into the cloud.

Question: What if the PC or Laptop I use to access the cloud dies, then what?

Our Answer: The beauty of the cloud is that you can use any device as an endpoint. We recommend that our clients keep one or 2 low-cost systems on hand to swap out dead or crashed systems. Of course, you can always pop down to Staples or Best-Buy and purchase a low cost PC or laptop in a pinch.

About our Founder

Greg's biggest passion is helping his clients get the dependability of a pencil and paper out of their modern day IT environments.

Growing up in the Greater Boston Area, Greg was surrounded by motivated business people during his youth. Naturally this lead to Greg wanting to someday run his own company where he'd be the one in control of the product and customer experience. While still attending College full-time, Greg opened up GH Microsystems and was designing networks and software for other small businesses during nights and weekends.

After falling in love with running his own business and working with other small business owners Greg decided to open T.O.S.S. Corporation (It used to mean "The Only Systems Solution"!) in 1985. TOSS spent its first 15 years doing standard IT and Network support. It was in 1999 when Greg decided to let the urge to buy a data center win out. That's exactly what he did. He got wind of an AT&T-owned data center going on the market and snatched it up before it even went up for sale. Greg has been leading TOSS in delivering Enterprise-class computing to small businesses ever since.

Greg is a graduate of the University of Rochester. As CEO of TOSS C3, he helps companies get out of the technology business by providing them with enterprise IT for a reasonable cost. Greg's philosophy is, clients are putting their critical IT function in our hands, so we must deliver a superior IT experience by consistently demonstrating security, reliability, and 24/7 support.

Greg is an award-winning, best-selling author of Sitting Duck, EasyPrey, You Can Conquer Your Bad Attitude and Computers Should Just Work!

He frequently speaks at NASDAQ, the New York City Bar and the Harvard Club of Boston and New York City. Greg is available for Keynotes, corporate and association events and training.

Greg also regularly appears on ABC, NBC, CBS and FOX TV. Talking Tech, Ransomware Prevention, Smartphone Addiction, Positive Mental Attitude and Smart Accessories for Pets.

You can find Greg at:
Greg.Hanna@TOSS.net
www.Twitter.com/GregHannaCEO
www.linkedin.com/in/GregHannaCEO
https://www.facebook.com/gregory.hanna.167

How to Contact TOSS:

Toll-Free:
1-888-966-9514

Main Phone:
1-508-820-2990

Office Locations:

Corporate Office
153 Northboro Road
Building 21
Southborough, MA 01772

Satellite Office
1253 Worcester Road
Framingham, MA 01701

TOSS C3

Cybersecurity | Cloud | Compliance ®

Your "Fix-IT-For-FREE" 100% Money Back Guarantee

If you are ever dissatisfied with any service for ANY reason, call and let us know. We will work with you to correct or repeat the service at no additional charge, or arrange for another engineer to repeat the service at no additional charge.

If this still does not resolve the issue to your complete satisfaction, we will refund 100% of the money you've paid us.

You'll notice we don't hide behind small print, legal-eeze, or other weasel clauses in our guarantee. That's because we are committed to excellence, your success, and completely confident in our ability to fix whatever problems you have and make you thrilled that you called us.

(888) 966-9514
www.TOSSC3.com

The Top 8 Reasons Why You'll Want To Work With Us

1. **We SPECIALIZE In Working With Fast-Growth Companies.** That means we understand your incredibly hectic and stressful work schedule and WHY it's critical to remove obstacles, frustrations and technical problems to keep you productive. We understand your desire to eliminate waste, extra steps, work-arounds and manual labor. We also have tech support available 24/7/365 since we know you don't work the normal "9-5" day, and can help you maintain the freedom to work remote while making sure you meet compliance standards for data security and backups.

2. **We Have The Unique Ability To Address Your Technology Needs – From Vision Through Long-Term Support.** We assist from vision to design and planning, to product specification through pricing and acquisition, to installation, implementation, documentation and project management, to post-project support of you and/or your users. This allows you to have one consistent team to work with that understands your environment, your people, how you work and your history, which means you don't have to waste time educating us.

3. **We Have A Team Of Certified Experts On Staff.** Unlike other IT firms, who have one or two guys trying to juggle multiple projects and wear various hats, we have teams of engineers on staff with diverse, specialized areas of expertise who work together to deliver the most effective and correct solutions to you. As a client, you are assigned to one of these teams. That means you'll always be able to get someone on the phone who knows YOU and understands YOUR environment and YOUR systems to provide helpful answers and quick resolutions of problems instead of having to talk to a complete stranger hundreds of miles away who knows nothing of you or your systems and wastes your time asking a lot of really dumb and annoying questions to try and "help" you.

4. **We Use Our Vendor Relationships To YOUR Advantage.** Having an advanced level of partnership with key vendors (Microsoft, VMware, Dell and Citrix) allows us access to special pre- and post-project assistance support levels that most "partners" do not have. We are able to provide the right solutions, priced right and validated by the vendor, so if any issues come up, we can get them resolved quickly and effectively.

5. **We Support Both On-Premise And Cloud Solutions.** Some IT firms won't offer or recommend lower-cost cloud solutions because THEY make less money. Our philosophy is – and always has been – to offer what's BEST for the customer, not us. That's how we keep so many customers long-term. We'll base our recommendations on what YOU want and what YOU feel most comfortable with. Our job is to lay out your options, educate you on the pros and cons of each and guide you to the best, most cost-effective solution for you.

6. **All Projects Are Completed As Agreed, On Time And On Budget.** When you hire us to complete a project for you, we won't nickel-and-dime you with unforeseen or unexpected charges or delays. We guarantee to deliver precisely what we promised to deliver, on time and on budget. We can offer our agreements on a fixed-fee basis so you know exactly what you're going to pay, not a penny more.

7. **We Have Flexible, Tailored-To-Your-Needs Support Options To Help You Better Manage Your Environment.** We provide our clients with a variety of managed support options, ranging from back-end maintenance and monitoring for issues, to user help-desk support with ticketing, to strategy and budget and asset/license life-cycle management. We have successfully provided these services for over 30 years and can create a solution specifically for you and your team.

8. **We Deliver Enterprise IT To The SMB.** After spending our first 20+ years focusing on delivering services to some of the largest and most successful companies in the world, we decided to cut the travel and focus right in our own back yard. We created the best-possible processes, practices and policies at the highest degree. We are now able to offer this level of service to the SMB market. We can provide any cybersecurity, cloud or compliance need you can come up with at a cost you can deal with. For small offices of 25 people and all the way up to 25,000 employees, TOSS loves making the Enterprise experience a realistic expectation for you and your firm.

 | +1.888.884.8677 | info@tossc3.com

The Readers Have Spoken

#1 in All 5 Technology Categories

TOSS C3 is The Undisputed Technology Company for Law Firms

Winners Work With Winners

2020 READER RANKING AWARDS — Reader Rankings — Lawyers Weekly — WINNER — Best IT Outsourcing

2020 READER RANKING AWARDS — Reader Rankings — Lawyers Weekly — WINNER — Best Cybersecurity

2020 READER RANKING AWARDS — Reader Rankings — Lawyers Weekly — WINNER — Best Data Recovery

2020 READER RANKING AWARDS — Reader Rankings — Lawyers Weekly — WINNER — Best Cloud Computing

2020 READER RANKING AWARDS — Reader Rankings — Lawyers Weekly — WINNER — Best Data Security

You Should Call TOSS Today

+1 (929) 254-0982

Thank you to all the loyal readers for your support.

TOSS® C³

Cybersecurity | Cloud | Compliance

www.TOSSc3.com | Greg@TOSSc3.com

Protection Against Ransomware. Guaranteed.

Ransomware is EVERYWHERE.

Judging by the headlines, today's cyber threat landscape is dominated by ransomware, a juggernaut of an attack that has claimed over $1B in extorted funds from organizations of all sizes, leaving many digitally paralyzed in its wake. Ransomware is evolving rapidly, with each new variant proving to be stealthier and even more aggressive than its predecessor. Organizations worldwide are scrambling to deploy better protection and further minimize financial risks of an attack.

New security technologies and more cyber insurance spend? What's wrong with this picture?

IT professionals and execs alike know that antivirus and static prevention do not effectively protect against targeted ransomware attacks, and are seeking out next-generation endpoint protection solutions. They are also simultaneously deepening their insurance coverage, as evidenced by a substantial upswing in cyber-insurance spending.

It takes valuable resources and hard-earned capital to procure and deploy the latest endpoint protection technologies. Shouldn't those solutions alone be effective enough to mitigate the risk of ransomware attacks without having to spend even more on insurance?

Zero-Day Protection: Ransomware Protection. Guaranteed.

TOSS C3 believes that your next-generation endpoint protection solution should give you complete confidence that your sensitive data is protected against ransomware and other sophisticated attacks—without the need for additional cyber insurance coverage.

In fact, we will guarantee it.

In an industry leading move, TOSS C3 is offering customers a guarantee that no ransomware attack will go undetected and cause irreparable damage.

TOSS C3 does not advise ransomware victims on whether or not to pay the ransom, but understands that there are times when it is necessary to recover data quickly. In the event that your organization must pay the ransom, ZPS Endpoint Protection Platform customers covered by the TOSS C3 ZPS Cyber Guarantee will be reimbursed up to $1,000 USD per affected endpoint if we're unable to keep you safe from a ransomware attack, and up to a maximum of $1,000,000 USD per company.

REQUIREMENTS

Required Zero-Day Protection Configuration:

- Quarantine: Enabled
- Cloud Validation: Disabled
- Cloud Intelligence: Enabled
- Latest Agent Version Deployed: Enabled

Required Operation System Configuration:

- Volume Shadow Copy Service: Enabled

Customer action when ransomeware is detected, but not blocked:

- Add threats to blacklist within one hour of infection notification
- Remediate and rollback within one hour of infection notification

Legal Terms & Conditions:

- Guarantee only covers the cost of the ransom, not hard business disruption or soft costs relating to PR/brand.
- TOSS C3 is not liable if paying the ransom does not lead to successfully recovering the data.
- Only Windows–based endpoints and servers with ZPS deployed on them will be covered under the guarantee.

Why Zero-Day Protection Service?

Last year, enterprise organizations collectively faced over three billion cyber attacks. When you consider the growing diversity and sophistication of these attacks, it's natural to wonder about how many of them you'll be able to prevent, and whether or not your organization's response is effective or timely enough.

Dealing with today's cyber threats requires a fundamentally different approach.

The truth is, static, AV-based solutions just don't cut it. Today's advanced malware, exploits, and other stealthy techniques now in use are blowing right by AV-based protection in a fraction of the time it takes to get updated with the latest threat signatures.

Furthermore, vulnerability exists in the gap between detection and response. Even if an attack is successfully detected, lack of integration with incident response tools forces manual attempts to neutralize it. In the meantime, that attack can still proliferate to other areas of your infrastructure.

The key to effective endpoint protection lies in the ability to dynamically analyze and detect any threat's behavior, and respond definitively at machine speed.

This is the essence of ZPS.

About Zero-Day Protection's Technology

The ZPS team was founded in 2013 by a group of cybersecurity experts who developed a fundamentally new, groundbreaking approach to endpoint protection.

ZPS unifies prevention, detection and response in a single platform driven by sophisticated machine learning and intelligent automation. With ZPS, TOSS can detect malicious behavior across all vectors of attack, rapidly eliminate threats with fully-automated, integrated response capabilities, and adapt your defenses against the most advanced cyber-attacks.

ZPS is a certified AV replacement.

TOSS C3
Cloud Conversion Company ®

For more information about ZPS and the future of endpoint protection, please visit: www.NeverPayaRansom.com | +1-888-966-9514