THE 7 MOST CRITICAL CYBER SECURITY PROTECTIONS EVERY BUSINESS MUST HAVE IN PLACE NOW!

Protect Your Business From Cybercrime, Data Breaches and Hacker Attacks

PANURGY
IT SERVICES ELEVATED

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are “low hanging fruit.” Don’t be their next victim!

This report will get you started in protecting everything you’ve worked so hard to build.

PROVIDED BY: PANURGY, LLC

AUTHOR: KEVIN GALLAGHER, PRESIDENT

3 Wing Drive, Suite 225
Cedar Knolls, NJ. 07927
973-400-3700
info@panurgy.com

About Panurgy

For over two decades, founding partners, Jeff Reingold and Kevin Gallagher, have worked to provide exceptional managed IT services to small- and mid-sized businesses with a need for high-quality technical support, but may lack the internal resources to handle it efficiently by themselves.

Panurgy offers a full range of expert, professional IT services to cover every stage of our clients business-technology life cycle. From assessment and design to implementation and sustained long-term management. We do all of this with an unshakable dedication, affordability, transparency, and with white glove customer care.

Technology Support for all your IT needs:

- Managed Services
- Security Solutions
- Cloud Solutions
- E-Mail/Spam Solutions
- IT Project Management
- Help Desk
- Desktop Support
- VOIP

www.panurgy.com
973-400-3700

PANURGY
IT SERVICES ELEVATED

Are You a Sitting Duck?

Your business is under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing and mobile devices, and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 7 security measures in place.**

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 web site or in an e-mail; once a hacker gain's entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (e-mails cleverly designed to look like legitimate messages from a web site or vendor you trust – or even from a key executive in your own company) is still a very common occurrence – and spam filtering and anti-virus cannot protect your network if an employee is clicking on and downloading the virus. That's why it's CRITICAL that you educate all of your employees on 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 slip-up; so constantly reminding and educating your employees is critical.

   On that same theme, the next precaution is implementing an Acceptable Use Policy (AUP). 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 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 employees 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 into 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's a company-owned device, you need to detail what an employee can and cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

We have sample, template AUPs we can provide to you to assist in starting to develop your own policies.

2. **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. An enforced, automated policy should require users to change their passwords at least every 45 days. 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.

3. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Flash or QuickTime, in addition to Windows itself; therefore, it's critical you patch and update your systems and applications when one becomes available. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

4. **Have an Excellent Backup.** 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 don't have 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, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; FULL backups should be taken multiple times per day around the clock – not just once per day or worse, and the backups should be regularly tested to confirm they can be restored. The worst time to test your backup is when you desperately need it to work!

5. **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 it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

But this trend 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); your 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 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 to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

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

6. **Don't Scrimp On a Good Firewall.** A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance.

7. **Protect Your Bank Account.** Did you know your COMPANY'S bank account doesn't 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 FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

So here are 3 things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY it happens can be stopped. If you discover even 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor your account 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 anti-virus software. And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. All of these things will greatly improve the security of your accounts.

Need Help in Implementing These 7 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll send one of our security consultants and a senior, certified engineer to your office to conduct a free **Security and Backup/Business Continuity/Disaster Recovery Audit** of your company's overall network health to review and validate potential data-loss and security loopholes. 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? 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?

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

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

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the many businesses 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 3rd 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.

You Are Under No Obligation to Do or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security and Backup/BC/DR Audit.** In fact, I will give you my personal guarantee that you will not have to deal with a pushy, arrogant salesperson because I do not appreciate heavy sales pressure any more than you do.

Whether or not we are a right fit for you remains to be seen. If we are, we'll welcome the opportunity. However, if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 973-400-3700 or you can e-mail me personally at keving@panurgy.com to get started.

Dedicated to serving you,

Kevin Gallagher, President
Web: www.panurgy.com
E-mail: keving@panurgy.com

Read What Our Clients Have Said About Panurgy:

"Panurgy's Total Data Protection saved significant data from being lost!"

Recently, **Ransomware attacked a PC on our network!** An entire volume on a shared drive was encrypted and the virus was spreading. Quickly, Panurgy removed the "host" PC from the network and was able to remove the infected files on the server. After the encryption files were deleted, Panurgy began a file restore of the files from our latest backup. We were up and running again quickly. Following this experience, **I am a believer in Panurgy's Total Data Protection.** We were able to avoid a potential loss of significant data, which could not have been restored if we did not have the backup data at the ready with Panurgy.

Mark Lysynecky, Controller - Garden State Growers

"If you do not want to worry about your network, choose Panurgy! They make your life easy."

"We have complete confidence that our network is fully functional and that whenever we have a network issue, it is fixed quickly and without drama. The engineers at Panurgy are extremely competent, have a wide range of knowledge and depth, so they can solve any issues that arise quickly and efficiently. They are my favorite vendor and always come through for us!"

Larry Taitel – Convertech

“We recently had our annual Penetration Test done by Digital Defense and received an “A” rating.”

“While using a 3rd party vendor to manage our Firewall and Backups, I lost faith as I noticed backups were not running every day and I wasn’t being notified along with several other things. In July of 2016, I contracted with Panurgy and have been extremely happy ever since. We recently had our annual Penetration Test done by Digital Defense and received an “A” rating. In the Penetration Test Executive Summary, Digital Defense said it best. “Persons responsible for maintenance and security of this node should be commended for the actions which resulted in the current rating.” Thank you Panurgy!”

George L. Duffy, Information Technology Supervisor - Pinnacle Federal Credit Union

“The single biggest benefit from working with Panurgy has been that I do not have to worry about my IT infrastructure.”

“Panurgy handled it all! The staff at Panurgy, has superior knowledge. There wasn’t a time when their team couldn’t figure something out. If you are on the fence about choosing an IT firm – DO NOT be penny wise and pound foolish. This was the best money I spent and gave me the peace of mind I needed to manage all the other aspects of my business.”

Sue Cohen – Negley, Assoc.

“Panurgy is always there when we need them!”

“With Panurgy we have seen 100% up time across our 3 locations! The communication with the techs, sales and management has always been responsive, patient and highly effective. If you need a long term relationship with an IT firm that is on-point all the time, there is no other choice – Panurgy is the best.”

Bill Moretti – Service Metal

“When you call you get a real person in USA (NJ) not a machine, not voice mails - a tech that knows you & your company! “

“With Panurgy, we have built history: They know our company & know what we need & what is important to us. They have worked with MBUSA & our other providers seamlessly. Funny but we have never worked with another IT firm.

For due diligence purposes, we did go out for bids a few years ago and decided to stay with Panurgy. The prices were in line & we knew what we had. **The grass is not always greener in the IT space!”**

Joseph Hobbs - Mercedes Benz, Princeton

ALEXIS BITTAR

“If you’re looking for a partner who is as dedicated to the success of your business as you, then look no further.”

“With Panurgy, we have an excellent partner with a strong technical team to support us which allows for our smaller internal team to focus on other initiatives. Panurgy’s technical knowledge is outstanding and the dedication to our company has been unparalleled.

If you’re looking for a partner who is as dedicated to the success of your business as you, then look no further. **Panurgy has assisted Alexis Bittar with rock solid recommendations, support and technical knowledge.** The staff is professional and resolves issues quickly & efficiently.”

Alexis Bittar – Ralph Bass

"Panurgy has helped lead us through the various issues and requirements of being 100% cloud-based."

"We also appreciate the 1x1 service of the help desk we receive from Panurgy.

Two things I feel Panurgy does better than any other IT support company:

1) Customer Service – whether it be the help desk, or the individual who is in our office bi-weekly, we appreciate the professionalism and knowledge of the techs that interact with our people; and

2) Panurgy has the ability to understand the IT needs of a growth company: – Panurgy helps Edge grow while maintaining a sophisticated IT infrastructure so that it's transparent to our employees yet continuously meets our needs in terms of performance and security.

I've actually talked to some of Panurgy's prospective clients on why choose Panurgy. I tell them the story of how the day before an important merger was going to close, our system went down. **Jeff got up in the middle of the night, drove >1hr to our office and got us back online. That's amazing customer service....Panurgy has been my go-to network IT partner ever since.**

I believe Edge is now the 5th company I've been involved with that uses Panurgy. They'll be the partner in the 7th, 8th and 9th as well if I get that opportunity."

Andy Einhorn - Edge Therapeutics

SJP | PROPERTIES

"We have been with Panurgy for 14 years and have no plans of leaving them! Throughout Super Storm Sandy they kept us up and running and have established a rock solid disaster recovery plan for our network."

"Panurgy's help desk is responsive and deals with the day to day issues at all of our sites in a timely manner. I have even had contractors that deal with them comment that they are a dream to work with compared to some. With 15 remote sites that Panurgy monitors, I can sleep at night knowing that if there are any issues, I will get an immediate call or email on any issues such as a site being down or intermittent problems.

From the sales team right up to the owners they are available when I need them. They always work to be part of the solution and not the problem. **Throughout Super Storm Sandy they kept us up and running and have established a rock solid disaster recovery plan for our network.** During Super Storm Sandy, Panurgy remained operational and assisted SJP in keeping our network up and running along with our back up site…without issue. We have been working with Panurgy for 14 years, they have always taken a positive attitude to resolve our problems.

I can't put the single biggest benefit of working with Panurgy since there are so many right at the top, so I will list them separately and you can use whatever you want.

- The help desk is second to none. The team is always polite and understanding with my staff when they call. And believe me some of my staff can be difficult."

- The sales team is always responsive to our needs and is always available to us. They continually make recommendations on how to better secure, operate, and maintain our network.

- The onsite service team is responsive and have a confident attitude.

- Several of our contractors that have to interface with Panurgy on network access for their equipment have come back to me and said that "Panurgy is one of the better IT service providers that they have worked with."

Gary Oravsky – SJP Properties

Brown & Brown INSURANCE®

“As an insurance company we tend to want to be cutting edge, not bleeding edge, and Panurgy have helped us maintain that balance.”

“We’ve been working with Panurgy for about 12 years and in that time they have never steered us wrong with regard to industry trends. To that end I would say that the single biggest benefit has been moving to new technology as it becomes available and, most importantly, stable.

Panurgy is reliable and will do whatever needs to be done to make something work properly, regardless of how long it takes or how difficult it is. I have heard from other branches of my company about their particular service providers who decide that something can’t be done and just bail on it. Panurgy doesn’t do that.

If someone was on the fence about choosing Panurgy as their IT firm, I would tell them: I am pretty passionate about uptime and I have worked with Panurgy for over a decade. Think about that, if Panurgy didn’t deliver quality service or keep my network up and running, I would be working with someone else.”

Rich Currie – Brown and Brown Insurance, LV

PANURGY
IT SERVICES ELEVATED