EZ MICRO
SOLUTIONS

7 SECRET ESSENTIALS OF SAFE COMPUTING

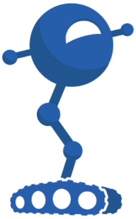
Safe computing is

everyone's responsibility

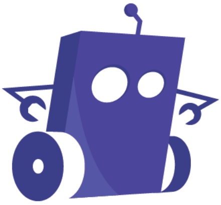
2670 Lehigh ST Whitehall, PA 18052 610-264-1232 ezmicro.com

7 SECRET ESSENTIALS OF SAFE COMPUTING

Did you know....



There were more than 1.46 million ransomware attacks detected in one year. That is 4,000 per day!



Most businesses are not "hacked". The bad guys are let in through the front door.

Cyber Security is *not* a computer problem—it is a human problem!

Concerned? Afraid? These scary and somewhat unknown facts are what inspired EZ Micro to create a book about safe computing.

610-264-1232
ezmicro.com

At EZ Micro, we believe it is everyone's responsibility for safe computing.

Let us show you how to stay safe.

Client safety is one of our top priorities at EZ Micro Solutions. In our journey to create a safe environment for our clients, we discovered important issues that we believe everyone should know.

With more than 25 years in business and the combined experience of thousands of hours among our professional IT staff, EZ Micro has put together important information that we hope you find to be of value to your organization.

If you have any questions along the way, always feel free to call us for help!

610-264-1232
ezmicro.com

SECRET #1
The Number 91

UNDERSTAND WHAT #91 MEANS TO THE SAFETY OF YOUR ORGANIZATION'S DIGITAL ASSETS

Why 91? Would you be surprised if I told you that over 50% of all hacks are from user error? What if I told you it's actually over 75%? Over 90%?

The first thing to understand about any safety or security issue is how to identify the real threat. It feels like everyday we hear another story about how a "hacker" cost another business millions of dollars through a cyber security breach. Are all of these events actually "hacks"? Let's look at an example.

A large municipality had its services effected for over 2 weeks. Law enforcement couldn't use the laptops in their patrol cars, the finance department couldn't pay their bills, security cameras were offline, and Microsoft was contracted for 1 million dollars in repairs to their system! How did this happen? Was it a hack? Was it a bad guy trying to get through a wall? **No.** It was a team member in the finance department who clicked on a **Word Document** attached to an email that was disguised as a payment voucher.

Over 91% of cyber-attacks begin with a team member clicking on something.

This kind of attack is commonly known as spear phishing. It is an increasingly common exploit with more specific and personal targeting. For example, a fraudulent message may refer to a specific team member by name, job position, or an actual business transaction that is going on in the organization.

The goal of a spear phishing attack is to trick the victim into either opening a malicious file attachment or clicking on a link to a malicious website often disguised as a legitimate one. This could open the door to compromise the network, steal information, induce a wire transfer, or hold the organization hostage (ransomware).

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How do I use the number 91 to protect my organization?

- Make sure you have current cyber security gear (most security-minded IT managers & technology firms implement up to 40 layers of security). Most experts agree that a **minimum of 20** security layers is normal.
- Find out if you need additional protection based on your industry and your compliance regulations. Up to 20 more layers may be required. Two of these layers include familiar tools such as Firewalls and Antivirus, but there are many more, depending on your organization's needs and your specific industry.
- Identify how many security layers your organization needs (consult with your IT manager or technology firm if needed).

SECRET #2
Understand the Difference

UNDERSTAND THE DIFFERENCE BETWEEN SAFETY CLIMATE AND SAFETY CULTURE

Would you ever step foot onto a construction site without wearing a hard hat? Of course not—they wouldn't let you near it! In the physical world, there have been major advances in safety and security for factories, construction sites, and healthcare facilities. Goggles, harnesses, helmets, gloves, scaffolding, and ladders, are all designed to keep us safe from bodily harm. However, every expert will tell you that none of these items are effective without safety awareness, training, and building a safety culture. Most businesses don't understand the **difference** between Safety Climate and Safety Culture.

Safety Climate

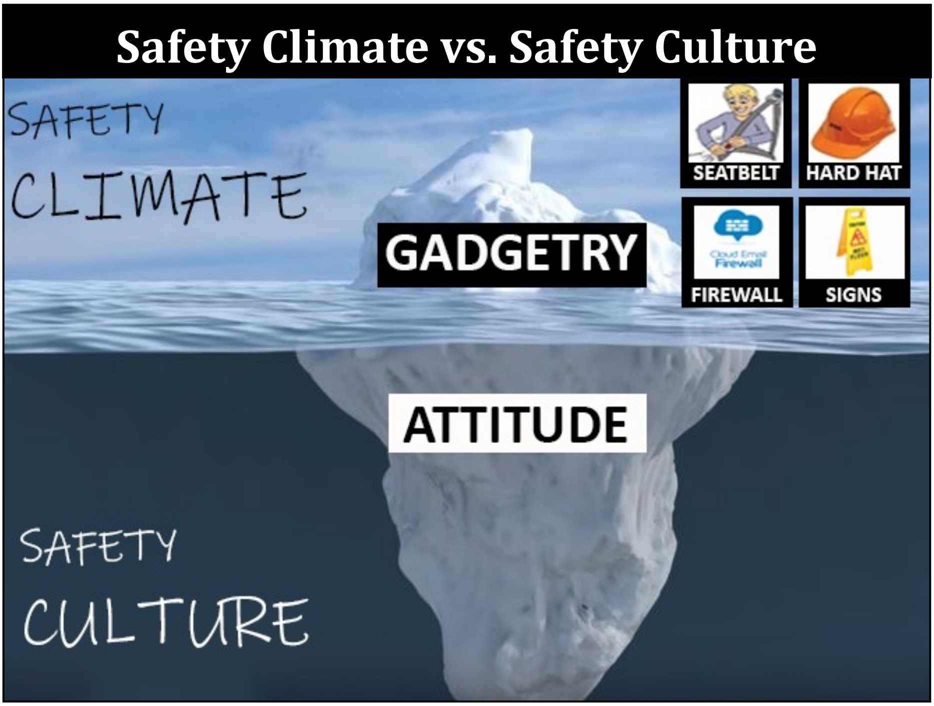
Safety climate features all the aspects of protection you can easily see. For cyber security, the safety climate would include file encryption, anti-virus software, a firewall, password complexity, etc.

Examples:

- Safety Director
- IT Director
- Antivirus Software
- Helmet
- Firewall
- Password strength
- Password expirations
- Safety Goggles
- Two-Factor Authentication
- Company Handbook
- Acceptable Use Policy
- Website Filtering
- Pain in the *[you know what]* IT Dept.

Safety Culture

This is the ongoing *philosophy* that informs all aspects of your organization's values and decision making. Unlike a safety climate that uses special products, gadgets, training, and implementation, safety culture is all about the philosophy of your organization. Company leadership has to model this behavior on a day-to-day basis. Like an iceberg, it's not what you see—*it's what you don't see*. It's more *attitude* than gadgets. It's consistent messaging that "this is way things are done around here."



Developing culture is one of the most complex things you will ever tackle. It's not about a new security layer or moving something from A to B—it's about the hearts and minds of your people.

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How can I identify my organization's safety climate and safety culture?

- Ask your Safety Director (if you have one) and your IT Manager to help you determine if a Safety Climate or Safety Culture exists at your organization.
- If you determine that you already have a safety culture, is there anything in place to measure its effectiveness?
- If you are having trouble answering these questions, ask your Safety Director and your IT Manager for help.

SECRET #3
If You Build it, They Will Come

IF YOU DON'T HAVE A SAFETY CULTURE, BUILD ONE. IF YOU HAVE ONE, APPLY IT TO THE OPERATION OF YOUR DEVICES.

How many times have you walked into a place that looks dirty or unsafe and you immediately turn around and walk out? Chances are, there is someone in charge with the attitude of "it's not my responsibility", "I can't fix it", or worse yet ,"I don't care". If you want to keep your organization safe, you need to take ownership and ***insist*** others follow.

"The Safety Culture of an organization is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and style and proficiencies of, an organizations health and safety management"

- Health & Safety Executive (HSE) Advisory Committee

Safety Culture is all about creating an environment where it is expected that "this is the way things are done around here." Without the appropriate culture in place, most employees see safety as something "management" is responsible for and not them. The employees believe management may "lecture" about safety, but that it is really the Safety Director's or the IT Director's job to keep them safe. In contrast, a Safety Culture inspires people at all levels in a company to see the consequences of their actions inside and outside the company.

Most importantly, safety doesn't come by just checking a box. There are all kinds of compliance authorities (OSHA, NIST, etc.), but the safest organizations are not the ones that view compliance requirements as a chore. Did you know that statistically the organizations that only utilize safety compliance often have the worst track records?

The most secure organizations have a safety culture in place. Everyone is trained from the executive suite down, and safety is in the forefront. In organizations with the best safety records, safety is not anyone's job, but rather everyone's responsibility. Safety conversations and training are an ongoing —not something that gets measured once a year to fill out a compliance checklist.

Sadly, many professions have no safety culture at all. Even companies that have strong safety cultures on the factory floor (construction and manufacturing) haven't applied the same philosophy to the office environment.

A great example is Joe the Iron Worker. Joe accepts employment at a construction company that specializes in steel structures. Before Joe is allowed to work on the site, he will receive days or even weeks of safety training. Even after all of his training, during Joe’s first week, he tries to “cut a corner.” This is so frowned upon that five of his co-workers stop him by reminding Joe how dangerous that is.

Compare that with training for a CPA firm. Ann the accountant is excited to begin her first day of work at the new Tax Firm. Will she typically receive safety training? No! Ann will probably work on her computer for months or even years before she ever receives any in-depth safety training.

Which company has the safety culture in place? Of course, it’s the iron workers, right?

Let’s take a closer look. The same company that trains their employees of all the dangers with construction doesn’t worry about the employees ***inside on the computers***. How much damage can they really do? In reality, the office employees can cost millions of dollars in losses by one...small…devastating…*click*.

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How do I build a Safety Culture or apply an existing one?

- Ask your Safety Director (if you have one) for help. For example, if you are a manufacturer and already have a strong safety culture on the floor, have your Safety Director work with your IT Manager to apply the existing culture to the operations of your computers, laptops, tablets and phones.
- Implement separate, ongoing training for management and the other departments as the type of training varies for each.
- Implement a *Safety Awareness Program* that measures awareness and safety records as well as offers training videos.

SECRET #4
Training, Training and More Training

PERFORM PROVEN & EFFECTIVE ANNUAL SAFETY CULTURE TRAINING WORKSHOPS

As mentioned above, the first step is to create and prescribe the proper training program for your management and executive teams. This is paramount, because how your executive team views and implements the safety culture will trickle down to the rest of the organization. Due to the fact that safety can vary so much from industry to industry and organization to organization, it is vital that your management and executive team training is well thought-out and implemented diligently.

Typically, management and executive team training will include some tactical training, but will focus more on strategy. Some of these strategic elements are the same as any other training in your organization.

- How do I get my team to buy-in?
- What are the incentives?
- How do I form the messaging?
- How do I build my initiative and wrap a positive, uplifting vibe around it?
- Am I going to get myself or a co-worker in trouble?
- How do I spot a threat?

- How do I receive training?
- What are my incentives?

Ask your Safety Director and IT Director to create an affordable training program to fit your needs. You may need to find an outside resource that specializes in these kind of training platforms.

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How do I build a Safety Culture training platform for my organization's executives and staff?

- Determine incentives.
- Ask your Safety Director, CIO, IT Director, or IT Firm to create an affordable training program to fit your needs.
- Find a third-party resource that specializes in these kind of training platforms.

SECRET #5
You Can't Have Too Many Signs

IMPLEMENT VISIBLE COMPUTER SAFETY SIGNAGE & MESSAGING TOOLS

We've all seen these iconic symbols in our daily lives so much that we can see them out of the corner of our eye and know to be careful. The signs immediately bring us back to training we received.

There are similar warnings present in your cyber security.   You may be ready to start implementing these guidelines, but what about the signage?   Just like in the physical world, we all need reminders to operate our devices safely.

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How do I implement cyber safety signage in my organization?

- Place the signs where my computer users work.
- Ask your Safety Director, IT Manager, or IT Firm to provide you and your staff with messaging tools that can be applied to computer login screens, break rooms, desks, tablets and phones.
- Talk to local business owners who have successfully implemented signs.
- Find out if your IT Firm provides these tools as a part of their package.

At EZ micro we developed stopthinkclick.org to help keep everyone safe:

STOPTHINKCLICK™.ORG

Safe Computing is Everyone's Responsibility

Sticky Notes

Mugs

Power Banks

Signs

610-264-1232
ezmicro.com

SECRET #6

Trust, but Verify!

INSTALL MEASURABLE, ONGOING, SECURITY AWARENESS TESTING AND TRAINING

This is one of the most important secrets of all...

You completed training, everyone has bought in, now everything will be perfect, right? Probably not. Even with the best intentions, people forget what to do. So what is the most effective way of making sure they remember? Testing.

How do you continually measure how prone your staff is to clicking on a malicious email or if they can identify a threat?   The answer is to implement a security awareness software platform. A properly configured platform will track your team members' click habits. In plain English, this will tell you what your employees click on. A good system will first create a baseline of your team's current habits. Then, it will send ongoing fake phishing email that tries to trick them into clicking on bad links.

If and when an employee clicks on something he or she shouldn't, they will be notified and directed to a short training video. The video is specifically designed to educate your team member on how to detect and report the threat the next time. This technique is then combined with robust reporting to management on each individual's habits as well as departments as a whole. A well-made platform also has levels of difficulty for the teams to scale, builds team comradery, and creates a positive, rewarding atmosphere in your workplace.

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How do I install a Security Awareness Program?

- Consult your IT Director or IT Firm. There are many platforms out there to choose from, or they might offer the curriculum for a monthly fee.

SECRET #7
Not All Insurance is Created Equal

PERFORM ANNUAL SAFETY REVIEWS SPECIFICALLY FOR YOUR CYBER INSURANCE

Yes, that's right. Insurance. While a company would never dream of leaving all of its assets uninsured, we don't always think about cyber insurance. We make sure our buildings, computers, and machinery are covered, but what about other exposure? We aren't used to insuring things we can't see.

In the early days of cyber security, we used to say, "Protect everything behind the firewall."   Before the days of the Internet, remote access, tablets, phones, and distributed workforces, everything was in one building and much easier to keep safe and secure. In fact, an IT Manager was somewhat like a security guard protecting from an intrusion.

This type of security approach does not apply anymore, because technology, habits, and even the expectations of our workforces have evolved. For this reason, there are so many more entry points for bad guys than just a set of computers in a building behind a firewall.

Some common vulnerabilities are:

- Email on laptops
- Tablets and phones
- Home computers remoting into company networks
- Social media

- Email addresses listed on websites

Organizational structures and cyber insurance require careful study and review. It is important to understand that most web developers and digital marketing companies are not security professionals and therefore need proper oversight.   There are many assets and vulnerabilities that are tied to your security landscape indirectly.

REMEMBER: Most web developers and digital marketing companies are NOT security experts

WHAT DO I DO NOW?

Suggested Steps to Make Changes in Your Organization

How do I properly conduct safety reviews of all the assets indirectly attached to my system?

- Have your IT Manager conduct an overall review of all devices with access to company data so you know where to begin.
- Understand and identify what social media is being used personally versus directly for your business. Each type of use carries its own security needs.
- **Review the information on your website.** Many companies have websites that give away information to criminals without any measure of its purpose for the business.   A good example is listing who is on the management team and providing everyone's email address.   Have a business person work with your IT Manager and web designer to review what information is actually needed to display on the website.

WHAT DO I DO NOW CHECKLIST

Now that you have read through the book, the following pages have a checklist for you to follow.

WHAT DO I DO NOW CHECKLIST

Now that you have read through the book, here are all the suggested items in one list.

Secret #1 Suggestions —How do I use the Number 91 to protect my organization?

- □ Make sure you have current cyber security gear (most security-minded IT managers & technology firms implement up to 40 layers of security). Most experts agree that a **minimum of 20** security layers is normal.
- □ Find out if you need additional protection based on your industry and your compliance regulations. Up to 20 more may be required. Two of these layers include such familiar tools as Firewalls and Antivirus, but there are many more depending on your organization's needs and your specific industry.
- □ Identify how many security layers your organization needs (consult with your IT manager or technology firm if needed).

Secret #2 Suggestions —How can I identify my organization's safety climate and safety culture?

- □ Ask your Safety Director (if you have one) and your IT Manager to help you determine if a Safety Climate or Safety Culture exists at your organization.
- □ If you determine that you already have a safety culture, is there anything in place to measure its effectiveness?
- □ If you are having trouble answering these questions, ask your Safety Director and your IT Manager for help.

Secret #3 Suggestions —How do I build a Safety Culture or apply an existing one?

- □ Ask your Safety Director (if you have one) for help. For example, if you are a manufacturer and already have a strong safety culture on the floor, have your Safety Director work with your IT Manager to apply the existing culture to the operations of your computers, laptops, tablets and phones.
- □ Implement separate, ongoing training for management and the other departments as the type of training varies for each.
- □ Director work with your IT Manager to apply the existing culture to the operations of your computers, laptops, tablets and phones.

Secret #4 Suggestions —How do I build a Safety Culture training platform for my organizations Executives and Staff?

- □ Determine incentives.
- □ Ask your Safety Director, CIO, IT Director, or IT Firm to create an affordable training program to fit your needs.
- □ Find a third-party resource that specializes in these kind of training platforms.

Secret #5 Suggestions —How do I implement cyber safety signage in my organization?

- □ Place the signs where your computer users work.
- □ Ask your Safety Director, IT Manager, or IT Firm to provide you and your staff with messaging tools that can be applied to computer login screens, break rooms, desks, tablets and phones.

- □ Talk to local business owners who have successfully implemented signs.

- □ Find out if your IT Firm provides these tools as a part of their package.

Secret #6 Suggestions —How to I install a Security Awareness Program?

- □ Consult your IT Director or IT Firm. There are many platforms out there to choose from, or they might offer the curriculum for a monthly fee.

Secret #7 Suggestions —How do I properly conduct safety reviews of all the assets indirectly attached to my system?

- □ Have your IT Manager conduct an overall review of all devices with access to company data so you know where to begin.

- □ Understand and identify what social media is being used personally versus directly for your business. Each type of use carries its own security needs.

- □ Review the information on your website. Many companies have websites that give away information to criminals without any measure of its purpose for the business. A good example is listing who is on the management team and providing everyone's email address. Have a business person work with your IT Manager and web designer to review what information is actually needed to display on

NOTES

EZ MICRO
SOLUTIONS

610-264-1232
ezmicro.com

EZ MICRO
SOLUTIONS

2670 Lehigh Street

Whitehall, PA
18052

610-264-1232