The Ultimate
CYBER SECURITY
Guide for Business

The Ultimate
CYBER SECURITY
Guide for Business

Page

What is Cyber Security?

Cyber security is one of those territories with strong vocabulary that can be intimidating at first. But it doesn't have to be. Just as with any other practice, it has ***layers of development***, which means you don't have to dig deep if you're not a technical person. Using the information that is relevant to you may be all you need. But as your business grows, your cyber security strategy should grow with it.

We're all familiar with the vulnerabilities of weak data security, but how many businesses really experience a data breach every year? According to ***Theft Resource Center*** and ***CyberScout***, the data risk management company reported the number of data breaches in the U.S. jumped 29% in the first half of the year, hitting a record high of 791. At least 15 security breaches occurred at separate retailers from January 2017 until now. Many of them caused by blemishes in payment systems, both online and in-store and taken advantage of by aggressive hackers; 80-90% of people that log into retailers' e-commerce sites are hackers using stolen data.

The ***ITRC/CyberScout*** report tracks data breaches divided into five categories:

Financial (Banking & Credit)

Health/ Medical

Government/ Military

Education

Business

The business sector remains with the highest percentage of total breaches reported- 54.7% at the six-month mark of 2018.

The healthcare industry ranked second and had a substantial increase from between 2016 to 2017- 22.6% to 30.7%. The education sector came in at third with 11.3%, followed by the financial industry with 5.8%, and the government/ military sector with 5.6%.

Cyber Security Metrics

Cyber security surveys affirm that 92% of business desire to have a well-designed cyber security plan, but only 20% are successful in executing one. Many companies aren't clear ***on the key guidelines to define metrics*** to assemble effective cyber security.

Cyber attackers are transforming their intelligence to launch attacks where many attacks go unnoticed. Security metrics assist IT security departments with tracking internal security policies, governance frameworks, and regulatory measures are following business needs, or not. Well-defined metrics can help security teams in accurately pinpointing the gaps in systems and weak links that are vulnerable to hackers. This productivity will improve the overall security and critically locate key drivers of security measurement.

> "Risk is a function of the probability that your organization will be involved in an attack and the harm that such an attack would cause."
>
> ***- David Strachan Morris, Pilgrims Group Limited***

What do Hackers Want?

Why doesn't cyber security get the respect it deserves? On average, 1.7 billion Americans are impacted by data breaches every year, and still, many companies have not embraced a corporate culture that includes privacy and security in their core values.

It's no surprise that hackers want money, but the mere thrill they get from entertainment may shock you. Some cybercriminals attempt to attack your enterprise for the challenge, while others are after institutional secrets for industrial and geopolitical espionage.

In 2015, Russian government-backed hackers got a hold of highly classified U.S. cyber secrets from the National Security Agency after a contractor transferred information to his home computer. Reported first by the Wall Street Journal, the theft included information on piercing foreign computer networks and protecting against cyber-attacks and is inclined to be considered one of the most significant security breaches to date and could enable Russia to bypass NSA surveillance and potentially penetrate U.S. networks.

https://www.reuters.com/article/us-usa-cyber-nsa/russian-hackers-stole-u-s-cyber-secrets-from-nsa-media-reports-idUSKBN1CA2DO

Frequently stolen information includes:

- Social Security Numbers
- Date of birth
- Email addresses
- Financial information
- Phone numbers
- Passwords

Most hackers acquire the ***information they can sell or use***. Stolen credit card numbers are at the bottom of the barrel these days because they are so easily accessible. Social security numbers are a main target- they are worth much more to identity thieves to commit miscellaneous crimes pretending to be someone else. Hackers can open new credit and bank accounts, commit tax fraud, access brokerage accounts, get medical treatment or even apply for various benefits. No identity theft is easily handled, but unlike a credit card that can instantly be closed, a Social Security number has a timeless shelf life.

> "Historic compromises have included small-to-medium size financial institutions, likely due to the less robust implementation of cybersecurity controls, budgets, or third-party vendor vulnerabilities," the alert continues. "The FBI expects the ubiquity of this activity to continue or possibly increase in the near future."
>
> ***- Krebs***

Health records are even more worthwhile because they're a data-rich market. In addition to enclosing Social Security numbers, they have medical history, date of birth, insurance information and perhaps the credit card used to cover co-pays. Many medical organizations have placed their focus on patient care and less on patient privacy and cybersecurity. They may not realize the value you of the data they collect.

Most Common Cyber Crimes

Monetary damages aren't the only concern for business owners and cyber crimes - data theft and breaches can tarnish a company's brand and customer reputation. No matter the industry, all business owners should be familiar with the multitudes of cyber-attacks for a better standing ground to prevent becoming a victim. Common cyber-attacks against businesses include:

▸ Malware

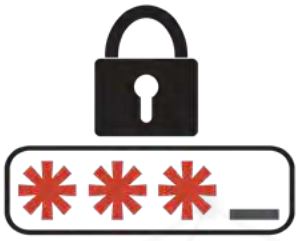
Malware is a term used to represent a variety of cyber threats like spyware, viruses, bots, trojans, and worms. It's code written with the intent to steal or destroy data on a computer or network. Malware is commonly introduced via email attachments, downloads or network vulnerabilities.

▸ Phishing

Phishing is the practice of sending emails disguised to be from trustworthy companies to lure people into revealing personal or classified information such as usernames, passwords, access links, credit cards numbers, etc. These emails often look legitimate with links to copycat websites where cybercriminals can steal any information procured.

▸ Password Attacks

Password attacks occur when third parties try to obtain access to computer systems or networks by cracking a user's password. These attacks don't usually involve any malicious software or code- instead uses the software on the attacker's computer that's capable of cracking passwords with information the attacker can provide.



- Denial-of-Service (DOS) Attacks

A denial-of-service (DoS) attackers focus on disrupting the service to a network. These attacks can prevent your business from accessing emails, websites, online accounts and any other services that your business may rely upon via computer. Attackers basically seize control of multiple computers and use them to generate high volumes of traffic or data streams through your network until it becomes too overloaded to function. The targets for this common cyber crime are usually large corporations or government sectors, but anyone can become a victim of having their computer hijacked. Without a proper monitoring system in place, many victims are unaware of DoS attacks.

The Cost of a Security Breach

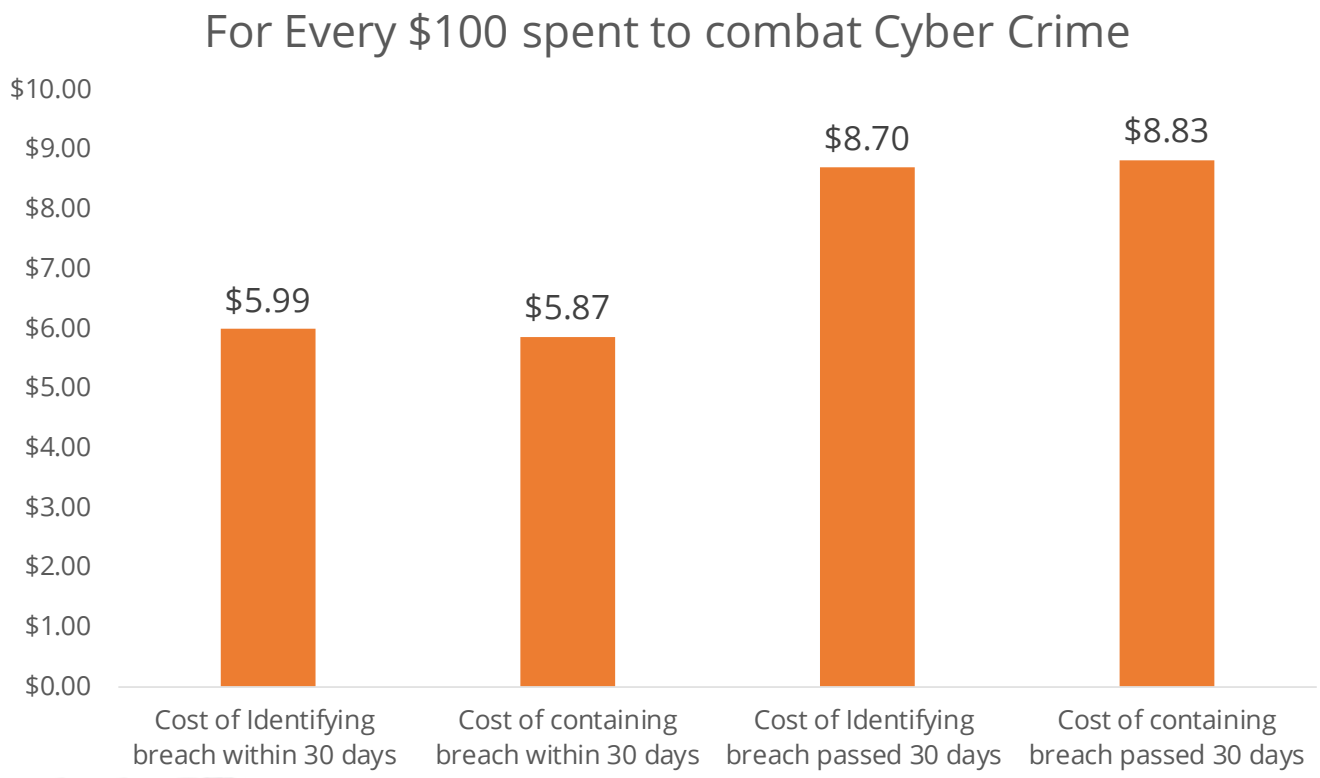
A data breach of any kind can hurt your business. The average cost of a data breach in the U.S. is $3.86 million in 2018-up 6.4% from the previous year (2017) according to the ***2018 Cost of Data Breach Report*** determined by ***IBM Security*** and Ponemon Institute.

On average, the cost of a compromised record is $225 but is significantly higher for exceptionally managed industries: healthcare ($380 per file) and financial services ($336 per file).

These figures include the direct costs of legal fees, notification, hiring additional staff and supplying identity monitoring services – including the loss of business that results from the breach. The impact to a company's reputation trailing a breach generally results in customers going elsewhere.

The Risk-Based Security report concluded the average time between discovering a data breach and disclosure is decreasing. It took companies an average of 82.6 days to disclose a breach in 2015. By 2017, this number was nearly lessened by half to 42.7 days and decreased even further to 37.9 days in the first quarter of 2018. This continuous improvement over the last four years is exactly the pattern we want to see in terms of cyber-attacks.

The longer a hacker goes undetected, the more damage they can do- which directly narrates with the volume of financial loss the company will battle. When a breach is spotted and contained in less than 30 days, the cost is nearly a million dollars lower, on average- breaches that took less than 30 days to contain averaged a cost of $5.37 million in 2017 but rose to $8.83 million for breaches that longer to contain. The General Data Protection Regulation (GDPR) enforces a 72-hour rule of notification for data breaches. Despite the steady year-to-year progress is decreasing disclosure times, organizations have a long way to go to meet the 72-hour requirement. Having a precise incident response plan in action can result in more than financial saving for your business.



So you can see early detection and remedies can save your business thousands.

How Reduce the Cost of Data Breaches

Outside of the patterns shown with a lower cost of a data breach in correlation with how quickly organizations identify and contain breaches- preparation and diligence pay. Studies found that incident response teams can lower the cost of a breach by as much as $14 per compromised record versus the average $148 per-capita cost. Multiple layers of security contribute to the cost savings- extensive use of encryption security can reduce cost by $13 per capita. There are many strategies to help businesses lower potential costs of a data breach.

Losing Your Customer's Trust Impacts the Total Cost of a Breach

Customers trust organizations with all information they harbor whether financial services or healthcare management. The ***data breaches in the past year*** caused organizations to lose customers, but businesses that worked to improve customer trust reduced the number of lost customers - resulting in reducing the cost of the breach. Customer loss also seemed to be minimized when senior-level leaders, like chief privacy officer (CPO) or chief information security officer (CISO) directed customer trust initiatives, again, decreasing the financial effect of a breach. Companies who lost less than 1% of existent customers acquired an average total cost of $2.8 million, while companies who experience customer loss greater than 4% lost an average of $6 million.

> "Ransomware shuts down 1 in 5 small businesses after it hits."
>
> ***-CNET.com***

Best Defensive Practices vs Cyber Crime

Employees as the 1st Defense

Hacking is the primary method of attack and accounts for 63% of all data breaches to date - according to the ITRC/CyberScout report - 9% caused by employee negligence or error. This contains inappropriate disposal of sensitive data and lost or stolen laptops or other devices. Incidental exposure on the web estimated 7% of the breaches.

Employees are on the front lines of information security. The more that can be done to regularly educate employees about the modest things to protect their devices can go a long way towards protecting the organization.

Cyber security policies are sets of guidelines that assist organizations in connecting and streamlining security efforts that are necessary to guarantee the protection of digital assets. They support business in identifying assets for protection, potential attacks on these assets, and measures taken to protect assets.

These policies list the responsibilities and consequences of the rights the users must abide by while working with business systems - including physical, individual management, hardware, and software. Cyber crimes reinvent themselves to explore vulnerabilities just as technology innovates, making cybersecurity policy audits a priority to be updated as needed.

Government and businesses are ranked the highest as top targets. It is imperative for every business to understand cybersecurity and its facets to reduce the possibility of cyber-attacks and breaches. A well executable security plan is what businesses need. Precise plans prioritize steps to be taken that defend the business network and data against most known attacks. Some steps may seem common and others beyond the capability of the average small business, but all are standards of effective cyber security.

> "When a cyber-attack happens, you won't be judged by it happening, but what you did when it happened."

Practical Cyber Security Checklist

- Train employees on cybersecurity threats
- Conduct a cybersecurity readiness assessment
- Discuss with your attorney how you might handle a ransomware attack
- Contact local law enforcement for their protocols for a ransomware attack
- Apply best practice multi-level password protocols
- Educate yourself at the Center for Internet Security

Cyber Security Insurance

Hacks, breaches, and network outages present more than just technical issues, and these potential consequences can lead business owners to adopt more sensible approaches to preventative measures and response plan security. Preventative measures help secure network defenses and employ security best practices. Response plans hold cybersecurity insurance designed as a safety net when a security incident occurs to ensure businesses recover after a cyber attack.

Cyber Security Insurance- sometimes mentioned as cyber liability or data-breach liability insurance- is standalone coverage. It's designed to help companies recover data loss from a security breach, network outage or service interruption. Cyber security policies are tailormade and vary depending on insurers because of prices and exclusions and are important to building a complete strategy for risk management and response.

Should You Purchase Cyber Security Insurance

No business is exempt from network outages or data breaches of any kind- small businesses and large enterprises alike. The impacts from financial loss lost business opportunities, damaged reputation and customer uproar can be devasting, and can potentially lead to loss of employment, as Target's former CEO discovered in 2014.

With so many extreme repercussions, cybersecurity insurance may be the knowledgeable thing to do for your business. It alleviates many of the costs and time put in investigating and resolving security mishaps and promptly assists your business with returning to normal operations.

What Types of Coverage Are Available

Cyber security comes in two types: first party and third party. Most insurers offer policies that combine features of both types, but you find few that don't. Business should be thorough when reviewing their cyber security policy to be aware of what is covered in the event of a security breach- most carriers will also include provisions and rejections into first or third-party policies.

A cyber security policy on first-party coverage will protect against:

- Losses suffered by the insured
- Damaged or lost digital assets, such as data or software
- Cyber extortion if the hacker holds insured's data for ransom
- Money stolen through and electronic crime
- Lost business opportunities or increased operational costs due to a disruption of the insured's computer

Cyber security policies on third-party coverage are typically geared towards third-party companies who manage networks, software or systems that hold compromised data.

Third-party coverage will cover the cost associated with:

- Security breaches of employee confidentiality
- Lost customer data and information
- Customer notification after a security breach
- Public relations efforts and battling defamation and intellectual property violations

What Kind of Cyber Security Insurance Do You Need

The most effective way to determine what kind of cyber security insurance your business needs is to complete a risk assessment and impact analysis. Businesses should review all their assets, including financial and customer data and intellectual property, then determine them as a high or low risk. Discover the main points of vulnerability during this process. Hackers are relentless and will exploit vulnerabilities in a system to steal a company's physical assets - the 2016 attack on Swift, once renowned for its highly secure financial message systems showed that cyber criminals will stop at nothing.

Business owners should visit with their legal team and other department heads for insight on the ramifications of a data breach and pinpoint which assets demand safeguarding when developing a risk-management strategy.

Phishing is Happening Right Now in Your Business (and how to prevent it from compromising your business)

With no knowledge, employees are tricked to undoubtingly giving access or sensitive data to hackers seeking to harm your business. Phishing (fish-ing noun) is a cyber crime where targets are contacted by telephone, text message or email by someone acting as a legitimate institution to convince people into providing sensitive data like personally identifiable information, credit card and banking details, passwords, etc.

Once the information is obtained, it is used to access valuable accounts and can result in identity theft and financial loss. Implementing your security measures does little to nothing if your employees are clicking malicious links they believe came from friends or clients- giving away the keys to your business. Phishers attempt to trick employees into installing malware or gain insight for attacks by claiming to be from IT. Train your employees not to hesitate to contact your IT department if they are receiving suspicious calls or emails. Besides email and website phishing, there is also 'vishing' (voice phishing), 'smishing' (SMS phishing) and various other phishing techniques hackers and cybercriminals are developing.

The first phishing lawsuit was filed in 2004 against a California teenager who created an imitation website for "America Online". He used this fake website to gain sensitive information from users and access the credit card details to withdraw money from their accounts.

Common Phishing Emails

Too Good to be True - Profitable offers and attention-grabbing statements are designed to attract people's immediate attention. Many will claim that a prize-winning of some sort like an iPhone, a vacation, a lottery, some lavish prize. If it seems too good to be true, it most likely is! Never click on any suspicious emails.

What's the Rush? – Popular tactic cybercriminals have in common is to urge you to "ACT FAST!" because the amazing deals are only for a limited time. Some will promote that you only have a few minutes to respond, some will tell you that your account will be suspended unless you update your personal information immediately. These emails are best to ignore. Reliable organizations give you substantial time to update any information needed, and will never reach out to users over an unsecured internet ad.

Hyperlinks – Links can act as the perfect disguise. Hovering over a link shows you the true URL the link will take you to upon clicking it. Usually, it will display a completely different site, or appear to be a popular organization's website with a misspelling; www.anericaonline.com – the 'm' is actually an 'n', so look closely.

Attachments – Attachments can be tricky. If you weren't expecting it, don't open it! Attachments often hold payloads like ransomware or other harmful viruses. The only file type that is always safe to open is a .txt file.

Unknown Sender – Everyone gets curious. Whether you receive an email from someone you do or do not know, if anything appears out of the ordinary, unexpected or suspicious, do not click on it.

It's imperative not to leak intellectual properties- not even accidentally. Cyber criminals go to great lengths to obtain sensitive data. Sharing a picture online with a whiteboard, documents or a computer screen in the background could reveal information that people outside of your company shouldn't see. IT departments are not consistently aware of all cyber threats, so immediately report any security warnings from your internet security software.

If working remote or traveling and plan on using the public wireless Internet, alert your IT department beforehand. If your company offers a Virtual Private Network (VPN), be sure to connect to it over any other network.

> "They'll just go after the user and they'll spray and pray. If you hit 100,000 email accounts and 10,000 hit the button and you're charging $200 a piece? That's a significant amount of income right there from doing very little."
>
> ***– Brett Callaughan, Malwarebytes Senior Systems Engineer***

Spear Phishing

Spear phishing is an email targeted at a specific individual, usually a person of higher power within the organization. Cyber criminals target higher-profile employees or business owners attempting to steal confidential information.

The attacker does research on their targets to find out who they regularly communicate with to send a personalized email that uses social engineering red flags, in attempting to get the target to click on a link or open an attachment.

email address of your significant other that has in the subject line: Honey, I had a little accident with the car, and in the body: I took some pictures with my smartphone, do you think this is going to be very expensive?"

For a spear phishing attack to arrive in the inbox of a target, the email is filtered through antivirus software on the target's computer. A non-extensive search on IT job boards for vacant system administrator positions at the target's organization can provide ample information to attackers. They often list the antivirus software including the version they use. If roadblocks come, DNX cache snooping and even social media give alternate information to find out. Once the antivirus is known, it's installed on a test bed to be sure the email comes through ok.

There are several ways attacks can get their hands-on email address from an organization and open source computer security projects that provide information about security vulnerabilities assists in penetration testing.

Internal Phishing

Your employees may be the weak link in your IT security. Cybercriminals bypass your firewall, encryptions, endpoint protection and other security measures by going after your internal employees. Phishing your employees and pinpointing the culprits is a logical course of action. Upon finding the bad fish, work out getting them through effective Security Awareness training that will keep them on their toes year-round. Train around that "one-click" that could compromise your business with:

- A simulated phishing attacks.
- Train your employees online about the various direction of social engineering.
- Send out simulated phishing attacks at least once a month.

Simulated Phishing Attacks

It's one thing to provide security awareness training, but another to know that the training has made a positive difference in your employee behavior. ***A simulated phishing program*** will test your employee's responses, allowing you to take immediate action if relearning is necessary. Simulated phishing attacks give you an individual assessment of employee jeopardy to phishing attacks and security awareness campaigns.

They can help you:

- Adapt future testing to employees are areas more at risk
- Meet compliance and regulatory requirements
- Reduce the number of employee clicks on malicious emails

Training your employees on social engineering and how to notice flaws in the authenticity of emails from fraudulent senders may be the low maintenance game changer in your cybersecurity protection.

> "Today's cybersecurity posture is not a onetime event but rather a state of mind, woven into the fabric of the business."
>
> ***– Ron Lenox, Cybersecurity Advocate***

Cyber Security Readiness

There are two types of breaches: One targets information, and one impacts physical security. Most breaches that disturbed organizations in 2017 were predominately informational. Although it's inconvenient and possibly harmful to a victim's financial status, the loss of information doesn't impact the physical safety of hacked victims. In 2018, it's predicted that breaches will impact victims physical and personal lives.

Countering cyber security is everyone's responsibility, so ***cyber security strengthening*** should be executed from both enterprise management and the workforce end. Companies invest millions of dollars in cyber security for an array of security products, but unless employees do their part, these investments have the potential to not be so effective. A Forbes study predicts that by 2021 cyber security expenses will reach one trillion dollars. Cyber security readiness and its components are vital for every business to understand to reduce the potential of cyber crime attacks.

Due to lack of well-designed security plans to secure digital assets from attacks, cybersecurity losses around the globe amount to a projected $400 billion a year. There are no limits when it comes to cyber victims; individuals, governments and business alike are all valuable targets. Enterprises are pressing to get cyber threat intelligence (CTI) to predict, detect and defend any cyber threat.

To develop a robust cyber security roadmap here is the not to miss checklist:

- Analyze the cybersecurity trends to keep your enterprise security policies updated.
- Keep conducting mock cyber-attacks also known as PEN testing (penetration testing) to check the employee response to cyber-attacks or to test the awareness gained from training sessions. (Facebook's security teams do send phishing emails to check the response of the employees to cyber-attacks).
- Keep cybersecurity insurance up-to-date.
- Develop industry current cybersecurity and information security policies.
- Audit all the business processes on regular basis to identify the significant risk areas. Also, keep the emergency response plan ready to handle any sudden risk incidents.
- Only allow secure remote access to data for users.
- Employee training on best security practices is required.
- Run a ***vulnerability assessment*** program on a frequent basis to detect any security defects in the network or IT infrastructure.

A proper cybersecurity plan connects critical information assets, commonly identified during a risk assessment, with essential business processes, goals and objectives that cybersecurity's require for their consistent operation.

For example, the business would identify its customer information database as an indispensable asset necessary to support operations of the organization. In conjunction, the cybersecurity plan would identify security practices and requirements necessary to protect the customer information database and the business processes it holds to.

What To Do When Your Business is Attacked

Contact Support

Before you get in over your head, call IT. Often what starts as a simple fix, can easily be made more complex by attempting to solve the problem on your own. Use authorized applications to access corporate data and sensitive documents. Study the process of how IT connects to your systems so that you aware of timeliness and when issues need to be resolved.

Preventing Phishing Attacks

For one reason or another, people can easily be fooled when it comes to online interactions. It's much easier to trick users, which is why phishing attacks are so excessive. There are countless potential consequences, and identity theft is in the thick of them. Even though hackers are constantly formulating new ways to get what they're after, there are some practices you can utilize to protect yourself and your organization:

- Spam filters can be used to protect against spam emails. Generally, spam filters evaluate the source of the message and the software used to send the message and its image to determine if its spam. Periodically, spam filters will block emails from authentic sources, so the software isn't always 100% accurate.
- Change your browser settings to prevent deceptive websites from opening. Bowers keep a list of fraudulent websites that will block the web addresses or send an alert message. The browser settings should only allow reliable websites to open.
- Most websites require users to enter login information with a user image displayed. These systems may open to security attacks. To maintain security, change passwords on a consistent basis, never using the same password for multiple accounts. For added security, use a CAPTCHA system for website logins.
- Hover over the URL of all links before clicking them. Secure websites with valid Secure Socket Layer (SSL) certificate will always begin with "https". In time, all sites will be required to have a valid SSL.
- Bank and financial institutions use monitoring systems to prevent phishing. Individual employees can report phishing threats, then legal actions can be taken against the fraudulent websites. Provide your employees with security awareness training to recognize potential threats.

Spoofing emails sent by cyber-criminals are disguised to appear to be sent by a business that offers services to the users. Most will not ask for personal information via email or threaten to suspend your account for any reason. Generally, banks and financial institutions will provide an account number or other personal details within the content of the email, which assures its source is reliable.

> "A whopping 91% of cyber-attacks and the resulting data breach begin with a spear phishing email."
>
> ***-Trend Micro***

Preparing Employees for Cyber Security Challenges

Observation shows that 30% of cybersecurity attacks are caused by employee error. ***Forrester research*** proposes that 70% of breaches are caused by employees' lack of cyber security awareness.

For example, browser plug-ins or add-ons you download can collect your information and pass it to the hackers. Something as harmless as an email appearing to be sent from your boss prompting you to click a link can create a path to hackers. The recent ***WannaCry Ransomware attack*** is one (phishing) attack where the email link opened caused extreme losses across enterprises.

This one click can raise the costs for your business in terms of reputation, finance, business data and loss of customer trust. Preparing employees for cyber attacks is the first line of defense.

To be sure your employees are ready and able to protect your business systems, ensure that they:

- Never click on a link or attachment in an email from an unknown source or from someone you did not expect to receive the email from.
- Ensure anti-virus, malware, and firewall software's up-to-date.
- For mobile devices keep track of them and use biometric authorization
- Never email sensitive files to your personal email. Best to access remotely when needed through a secure connection.
- Use up-to-date security practices and anti-virus and browsing security software at home and for personal devices.
- Do not browse on sites that force the sharing of information or are of a non-professional nature because just visiting can open you up to hackers.

Cyber crimes happen everywhere. You need to protect your business by working towards prevention. It is important for every business to understand cyber security and its components to reduce attacks. Want to dig a little deeper to know how ready your business is to fight cyber crimes, here is a free assessment from our experts.