January 2023

TechTidbit.com

brought to you by Tech Experts

# What Are The Top Cybersecurity Attack Trends For 2023?

*Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.*

As the world becomes increasingly reliant on technology, cyber attacks have become a major concern for individuals and organizations alike. In 2023, it is likely that we will see a continuation of current trends, as well as the emergence of new threats. Here are some things to look out for:

## Ransomware attacks

Ransomware attacks involve hackers encrypting a victim's data and demanding a ransom in exchange for the decryption key. These attacks can be extremely disruptive, as they can prevent businesses from accessing important data and systems.

It is likely that we will see an increase in the number of ransomware attacks, as well as more sophisticated and targeted attacks.

## Phishing attacks

Phishing attacks involve hackers sending fraudulent emails or messages that appear to be from legitimate sources in an attempt to steal sensitive information, such as login credentials or financial data. These attacks are often difficult to detect, as the attackers use increasingly sophisticated methods to make their messages appear legitimate.

It is important to be wary of any unsolicited emails or messages, and to verify the authenticity of the sender before clicking on any links or providing personal information.

## Supply chain attacks

Supply chain attacks involve hackers targeting the supply chain of a company in order to gain access to the company's systems and data.

This can be done through the use of malicious software that is introduced into the supply chain, or through the compromise of a third-party vendor or supplier. Companies should carefully vet their suppliers and have robust cybersecurity measures in place to protect against these types of attacks.

## IoT attacks

The Internet of Things (IoT) refers to the interconnected network of devices that are connected to the internet, such as smart thermostats, security cameras, and smart appliances.

These devices can be vulnerable to cyber attacks, as they often have weak security measures in place. Ensure that your IoT devices are properly secured, and to be wary of any suspicious activity on these devices.

## Cryptojacking

Cryptojacking involves hackers using a victim's computer or device to mine cryptocurrency without their knowledge or consent. This can result in the victim's device becoming slowed down or unusable, as well as the potential for financial loss.

## AI-powered attacks

Artificial intelligence (AI) has the potential to revolutionize the field of cybersecurity, but it also presents new opportunities for attackers.

We may see the emergence of AI-powered attacks, in which hackers use AI to automate and scale their attacks. It is critical that individuals and organizations are aware of this potential threat and to take steps to protect against it.

To protect against these and other cyber threats, you need to implement robust cybersecurity measures, such as using strong and unique passwords, regularly updating software and security protocols, and using security software to protect against malware and other threats.

It is also important to be aware of the potential risks and to be cautious when online, as well as to educate others on how to stay safe online. By being proactive and vigilant, we can help to mitigate the risks of cyber attacks and keep our data and systems secure.

To protect against these and other cyber threats, you need to implement robust cybersecurity measures, such as using strong and unique passwords, regularly updating software and security protocols, and using security software to protect against malware and other threats.

# What's Changing In The Cybersecurity Insurance Market?

*"No one is safe. Even small businesses find they are targets. They often have more to lose than larger enterprises as well."*

Cybersecurity insurance is still a pretty new concept for many SMBs. It was initially introduced in the 1990s to provide coverage for large enterprises. It covered things like data processing errors and online media.

Since that time, the policies for this type of liability coverage have changed. Today's cyber insurance policies cover the typical costs of a data breach including remediating a malware infection or compromised account. Cybersecurity insurance policies will cover the costs for things like:

- Recovering compromised data
- Repairing computer systems
- Notifying customers about a data breach
- Providing personal identity monitoring
- IT forensics to investigate the breach
- Legal expenses
- Ransomware payments

The increase in online danger and rising costs of a breach have led to changes in this type of insurance.

No one is safe. Even small businesses find they are targets. They often have more to lose than larger enterprises as well.

The cybersecurity insurance industry is ever evolving. Businesses need to keep up with these trends to ensure they can stay protected.

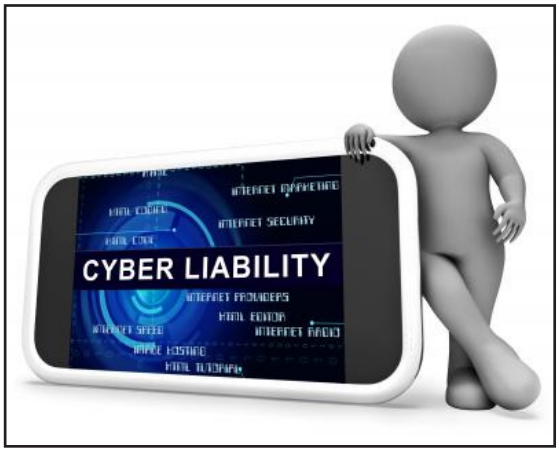
## Demand is going up

The average cost of a data breach is currently $4.35 million (global average).

In the U.S., it's more than double that, at $9.44 million. As these costs continue to balloon, so does the demand for cybersecurity insurance.

Companies of all types are realizing that cyber insurance is critical. It's as important as their business liability insurance.

With demand increasing, look for more availability of cybersecurity insurance.




## Premiums are increasing

With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up. In 2021, cyber insurance premiums rose by a staggering 74%. Insurance carriers aren't willing to lose money on cybersecurity policies.

## Certain coverages are being dropped

Certain types of coverage are getting more difficult to find. For example, some insurance carriers are dropping coverage for "nationstate" attacks. These are attacks that come from a government.

Many governments have ties to known hacking groups. So, a ransomware attack that hits consumers and businesses can very well be in this category.

In 2021, 21% of nation-state attacks targeted consumers, and 79% targeted enterprises. So, if you see that an insurance policy excludes these types of attacks, be very wary.

Another type of attack payout that is being dropped from some policies is ransomware.

Insurance carriers are tired of unsecured clients relying on them to pay the ransom. So many are excluding ransomware payouts from policies. This puts a bigger burden on organizations.

## It's harder to qualify

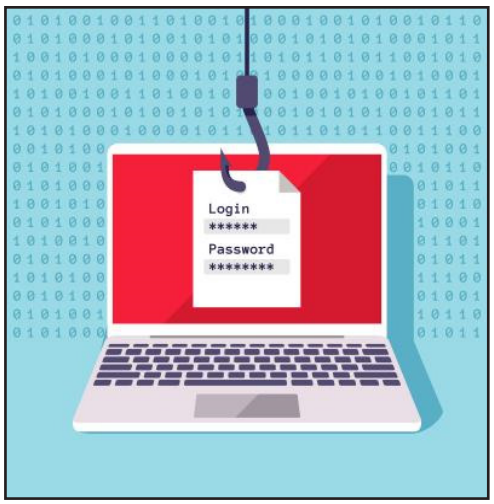
Just because you want cybersecurity insurance doesn't mean you'll qualify for it. Qualifications are becoming stiffer. Insurance carriers aren't willing to take chances. Especially on companies with poor cyber hygiene.

Some of the factors that insurance carriers look at include:

- Network security
- Use of things like multi-factor authentication
- BYOD and device security policies
- Advanced threat protection
- Automated security processes
- Backup and recovery strategy
- Administrative access to systems
- Anti-phishing tactics
- Employee security training

# Business Email Compromise (BEC) And Phishing Are Dangerous For Small Businesses

Business email compromise (BEC) and phishing are two of the most common and damaging cyber threats facing businesses today. BEC involves the fraudulent use of email to impersonate a legitimate business or individual in order to gain access to sensitive information or financial resources.




Phishing, on the other hand, is a type of cybercrime that involves the use of fraudulent emails or websites to trick individuals into revealing sensitive information, such as login credentials or financial information.

BEC attacks often target employees with access to sensitive financial information or those who have the authority to make wire transfers or other financial transactions.

The attackers use sophisticated social engineering tactics to trick the employee into revealing login credentials or other sensitive information, or to convince them to make a financial transaction on behalf of the company. In some cases, the attackers may even impersonate a high-level executive or vendor in order to gain the trust and cooperation of the employee.

One of the most common tactics used in BEC attacks is the "man-in-the-middle" attack, where the attacker intercepts legitimate emails and alters them to redirect payments or other financial transactions to their own account.

Other tactics include the use of fake invoices, purchase orders, or other financial documents to trick employees into making payments to the attacker.

Phishing attacks, on the other hand, generally aim to trick individuals into revealing sensitive information or clicking on malicious links. These attacks often take the form of fake emails purporting to be from legitimate organizations, such as banks or government agencies, and may contain links to fake login pages or download malicious software onto the victim's computer.

To protect against BEC and phishing attacks, it's important for businesses to implement strong security measures and to educate their employees on how to spot and avoid these threats. Some best practices for protecting against BEC and phishing attacks include:

- Implementing strong email security measures, such as spam filters and email authentication protocols, to help identify and block fraudulent emails.
- Training employees on how to spot and avoid phishing and BEC attacks, including teaching them to be wary of unsolicited emails and to verify the authenticity of any emails requesting sensitive information or financial transactions.
- Establishing strong passwords and using two-factor authentication to protect login credentials and other sensitive information.
- Setting up monitoring systems to detect and alert on unusual or suspicious activity, such as unexpected wire transfers or login attempts.
- Regularly updating software and security protocols to ensure that the latest security measures are in place.

In addition to these measures, it's important for businesses to have a plan in place for responding to a BEC or phishing attack. This should include:

- Establishing a clear chain of command for reporting and responding to suspicious activity.
- Designating a team to investigate and respond to potential attacks.
- Having a process in place for assessing and mitigating the damage caused by an attack.
- Reviewing and updating security protocols on an ongoing basis to ensure that they are effective in protecting against these threats.

Overall, BEC and phishing attacks are a serious threat to businesses of all sizes. By implementing strong security measures and educating employees on how to identify and avoid these threats, businesses can protect themselves and their customers from these damaging cyber attacks.

*"BEC attacks often target employees with access to sensitive financial information or those who have the authority to make wire transfers or other financial transactions."*

**Contact Information**

**Tech Experts Support Team**
(734) 240-0200
support@MyTechExperts.com

**Main Office**
(734) 457-5000
info@MyTechExperts.com

**Sales Inquiries**
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

**15347 South Dixie Highway**
**Monroe, MI 48161**
**Tel (734) 457-5000**
**Fax (734) 457-4332**
**info@MyTechExperts.com**

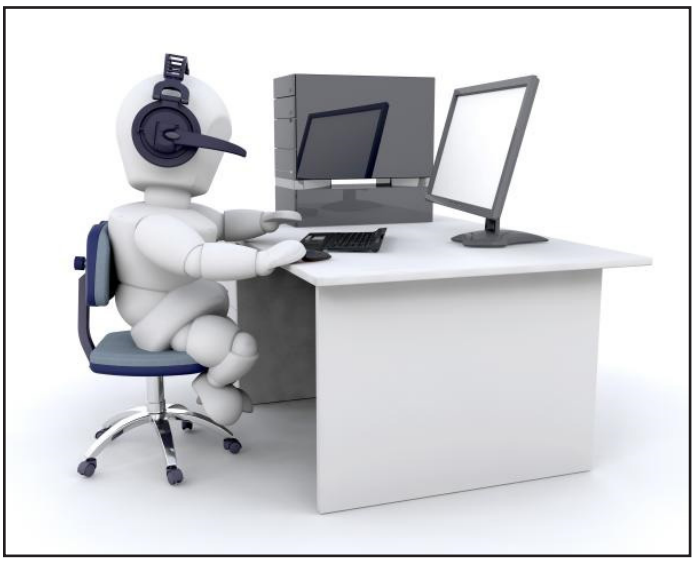


# Why Should Your Business Consider VoIP?

Voice over Internet Protocol (VoIP) phone service is a popular choice for small businesses because it offers a range of benefits that can help improve communication and increase productivity.

In this article, we'll take a look at some of the key advantages of using VoIP phone service for small businesses.

One of the biggest benefits of VoIP phone service is cost savings. Traditional phone systems often require expensive hardware and installation fees, as well as monthly charges for long distance calls.



VoIP phone service, on the other hand, uses the internet to make and receive calls, which means there are no additional charges for long distance calls. This can be a major cost saver for small businesses with employees or clients in different locations.

In addition to cost savings, VoIP phone service also offers flexibility and convenience. With VoIP, you can make and receive calls from any location with an internet connection, which means you can stay connected even when you're on the go.

This can be especially useful for small businesses with remote workers or those that need to stay connected while traveling.

VoIP phone service also offers a range of advanced features that can help improve communication and increase productivity. For example, many VoIP providers offer call forwarding, which allows you to automatically redirect incoming calls to another phone or voicemail. This can be particularly useful for small businesses that may not have dedicated receptionists or that need to manage calls outside of normal business hours.

Another useful feature of VoIP phone service is the ability to use virtual numbers. This allows small businesses to have a local presence in different areas, even if they don't have a physical location there. This can be particularly useful for businesses that want to target customers in different regions or that want to make it easier for customers to reach them.

VoIP phone service also offers the ability to integrate with other business tools and applications. For example, many VoIP providers offer integration with customer relationship management (CRM) systems, which can help small businesses keep track of customer interactions and improve their overall customer experience. Other integrations, such as the ability to send text messages or make conference calls, can also help small businesses stay connected and collaborate more effectively.

Finally, VoIP phone service is generally easy to set up and use. Most providers offer simple plug-and-play devices that can be easily connected to an internet router, and many offer online portals that allow users to easily manage their accounts and make changes to their settings. This can be particularly useful for small businesses that may not have IT staff or that want to minimize the time and effort required to manage their phone systems.

In conclusion, VoIP phone service offers a range of benefits for small businesses, including cost savings, flexibility, advanced features, and ease of use. By switching to VoIP, small businesses can improve their communication and increase productivity, while also enjoying the convenience and cost savings that come with using internet-based technology.