

ResTech Solutions | Houston, TX
713-936-6855 | info@restech.solutions |
<https://restech.solutions>



Cybercrime: A Global Perspective

Ransomware: The Cyber-Threat
Terrorizing the World

How to Defend Your Business from
Daily Threats



ResTech Solutions BRINGS YOU

Cybersecuring Our Future

QUARTERLY
ed. 1 - Q3 2022

04

INTRODUCTION

Who we are and what we
bring to you

08

CYBERCRIME

A global perspective of both the
modern threat and security
landscape

11

CONFIDENTIAL DATA

Protecting your intimate
information in today's landscape

13

DIGITIZATION

Why it's never going away or
slowing down, and what you can
expect from the future

16

RANSOMWARE

The cyber threat terrorizing the
world



30

CYBER-DEFENSE

How to defend your business from daily threats

32

RISK

MANAGEMENT

Best practices for mitigating cyber risk

37

THE BEST DEFENSE

How to defend your business from daily threats

44

CYBERSECURITY NEWSLETTER

Get more frequent cybersecurity updates and news to help your business

45

TESTIMONIALS

See what our clients have to say about us



INTRO DUCTION

Hi,

The digital world is everywhere, and hard to understand! Don't you sometimes wish that you had a handy guide for what was going on in the world of new technologies?

Online technology has the unique privilege of making extremely big strides in a short period of time. Think about the state of the internet when you were born versus where it's at today. Pre-internet days and old dial-up computer users remember how it was before smartphones were in every pocket, tracking your every move and helping people navigate every aspect of their busy, modern lives.

It's a phone, camera, calendar, email, game and browser all rolled into one. You can literally access any information you want at any given time. How many times have you touched your phone in the past hour?

For better or worse, technology is here to stay. That's why this magazine is launching, to bring you the latest news about cyber-threats, and the legislation and security features that are coming out to combat these dangers.

How is the landscape of cybersecurity changing? That's what we're here to investigate for you.

LET'S GET STARTED

ABOUT



who is ResTech Solutions?

Hi! Cybersecurity expert, David Levine, bringing you the latest in cybersecurity news and events.

First, I want to thank you for picking up this magazine and joining the fight against cyber-threats to you and your business! Education is the first (and most important) step toward preventing insider and outsider threats from attacking your personal data.

That's what we do here at ResTech Solutions, along with our standard IT services to help keep your business running and secure.

Bringing you this magazine every quarter is my way of bringing accessible cybersecurity tips and industry knowledge right to your front door — or your coffee table.

For a sense of cybersecurity now and going forward, here is Cybersecuring The Future Quarterly.

DAVID LEVINE
FOUNDER & CEO



WHEN I GOT LOCKED OUT OF MY COMPUTER RESTECH PROVIDED ME WITH PEACE OF MIND AS THEY WERE ABLE TO RECOVER ALL MY IMPORTANT DATA AND SET UP AN ENCRYPTED CLOUD BACKUP SOLUTION TO PROTECT MY DATA.

- JAMES LI



"There's no silver bullet solution with cybersecurity. A layered defense is the only viable defense."

- James Scott, Institute for Critical Infrastructure Technology

CYBER CRIME:

A Global Perspective

The world is becoming more in tune with cyber-crime and -security. The more we learn about what threats exist, the better prepared we can be to stop them before they breach our security structure.

The "Dark Web" refers to that underbelly of the internet where people in crime shows go to for hitmen and illegal weapons -- but there's much more to it than that. It's also a place for cybercriminals to trade intelligence and software to help each other pull off their crime of choice. If you know where to go, you can buy malicious codes, ransomware kits, malware-as-a-service, and other threats that are ready-made for criminals to unleash on victims.

These days, cybercriminals don't have to be expert hackers themselves. That's why online marketplaces hosted on the darknet are so dangerous: Anyone with money and know-how can arm themselves with cyber-threats, and even get advice on how to use them. People review businesses and browse around just like legitimate online shopping.

Recent success has come in the global fight against online threats, though. Hydra Market, one of the biggest hubs on the Dark Web for illicit activity, was recently dismantled by US and German investigators working together to bring down what used to be the world's biggest dark cyber-marketplace.

The Hydra marketplace catered mostly to Russian cybercriminals, and was the hotspot where 80% of crypto exchanges on the dark web took place in 2021. It was, until recently, the largest and oldest dark marketplace online, operating since 2015 until April 2022.

Hydra charged commission on all transactions made on their servers and they only operated in cryptocurrency. Since Hydra's inception, it's been the source of \$5.2B cryptocurrency transactions. At the time of its closure, German officials secured \$25M in bitcoin from Hydra's servers.

”
HYDRA
WAS...THE
MOST
LUCRATIVE
AND
PROLIFIC OF
ITS KIND



The Hydra servers previously facilitated the purchase and sale of illegal goods and services, including:

- Cryptocurrency
- Identifying credentials and PII
- Financial information
- Money laundering
- Hacking starter kits, and
- much, much more.

It's not the only dark net marketplace on the planet, though Hydra was certainly the most lucrative and prolific of its kind previous to its seizure.

The successful elimination of the Hydra servers and subsequent arrest of an important administrator will bring awareness to the prolific nature of the dark web, which will ideally propel more businesses to invest in defensive services. It is possible to defeat these underground marketplaces and protect private data on a global scale.

BUT WAIT!

Don't be too afraid of evolving cyber threats.

That's why cybersecurity experts are CONSTANTLY hard at work to bring you safety measures that address newfound digital dangers to you and your company's private data.



a new era

PROTECTING CONFIDENTIAL DATA

Much of the time when you're hearing about cybersecurity, your mind jumps to password protection and those seemingly-endless phishing trainings that your HR department keeps sending out. However, it also includes a wider ecosystem of legal regulations, common business practices and knowledgeable end-users which all work together to keep your personal and professional information safe.

For example, banks are now set to experience the next mass cybersecurity reform. This spring, American banking institutions will have to meet new standards of transparency and response when it comes to cyber threats.



Fast action must be taken whenever a breach or corruption is discovered, so that you can locate and expel the threat before files are corrupted or stolen. Banks deal with some of the most important and private information that we access through the web: Our money. That's why they will soon be required to report significant attacks within 36 hours and notify any customers whose information might have been accessed or compromised in the attack.

This is a change from previous reporting standards, which only required transparency when it came to the unauthorized access of customer information. Now banks will also have to tell customers about threats that cause general outages, technical issues or disruptions that affect their ability to use the service. All of this is in addition to the expectation that these banks will implement stronger defenses to avoid many of these issues in the first place.



DIGITIZATION NEVER STOPS

Despite current cyber protections and security regulations, increased digitization continues to spur bad actors to invent more complex threats that they can weaponize against businesses like yours. Thus new regulations are coming out, and will continue to evolve, to keep customers and banking institutions (and every other industry) safe from these threats.

”

THESE NEW
REGULATIONS WILL
FORCE BANKS TO
IMPROVE ON THEIR
ALREADY-TIGHT
SECURITY TO
GUARANTEE OUR
FINANCES STAY BOTH
SECURE, AND EASILY
ACCESSIBLE TO US.



The overall aim is to get more banks investing in their cybersecurity, however that looks for their particular business. Data breaches are only becoming more common and our financial institutions need the cybersecurity posture to defend against the evolving threat landscape.

Banks currently still face threats from:



- Unsecured data
- DDOS or DOS attacks
- Malware and ransomware
- Unencrypted third party services
- Weak passwords
- Website spoofing
- Data wiping and/or theft

Thus, opportunities for victimization abound. This is part of the reason why banks are already among the biggest investors in cybersecurity. 95% hire a chief information security officer (CISO) or chief security officer (CSO) already. These institutions also tend to utilize strong cyber insurance policies, in part because financial theft is so rampant. After all, stealing money itself is much faster than hawking stolen goods on the Dark Web.

These new regulations will force banks to improve on their already-tight security to guarantee our finances stay both secure, and easily accessible to us.





"Attackers are using the noise of ransomware to their advantage, as it provides the perfect cover to distract attention so they can take aim at their real target: exfiltrating IP, research and other valuable data from the corporate network."

- Matt Lock, Help Net Security

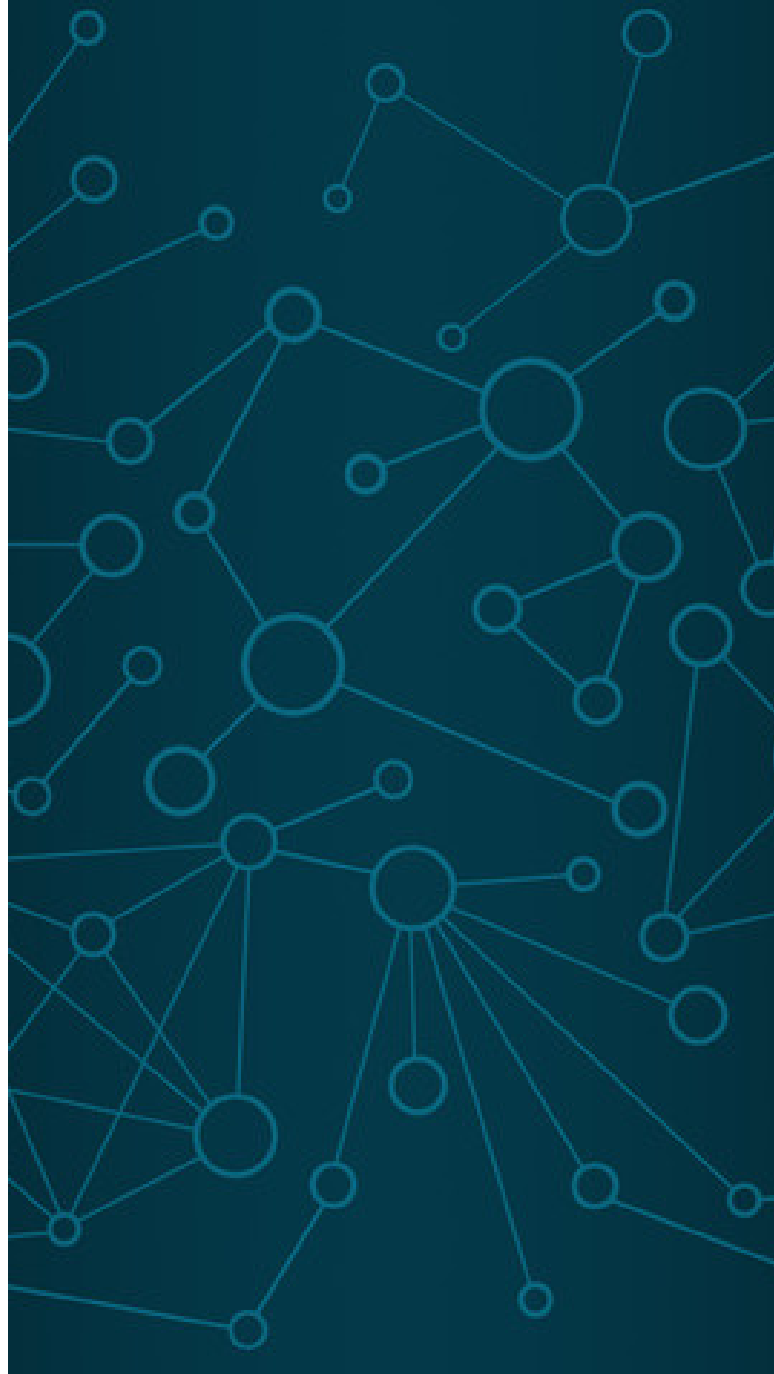
RANSOM- WARE:

*the cyber threat
terrorizing the
world*

In recent years, ransomware has become more and more of a threat to businesses of all sizes, from small companies to huge corporations. This kind of cybercriminal sees the benefit of a payday on top of whatever they can sell the stolen files for. The way that ransomware has progressed on the Dark Web now has cybercriminals selling their codes to other cybercriminals, for them to employ against the business of their choice.

RaaS, or ransomware-as-a-service, is one of the reasons that this threat type has risen so drastically in recent years. RaaS is effectively packaged code that the Dark Web seller puts up for as little as \$10. These are, of course, very basic codes that will nonetheless infiltrate the target business and launch the ransomware onto their system as intended.

Less affordable options can total over \$100, and the very advanced versions go for thousands on the Dark Marketplace. You can imagine the defenses, capabilities and demands that come with a pricey bit of code like that.

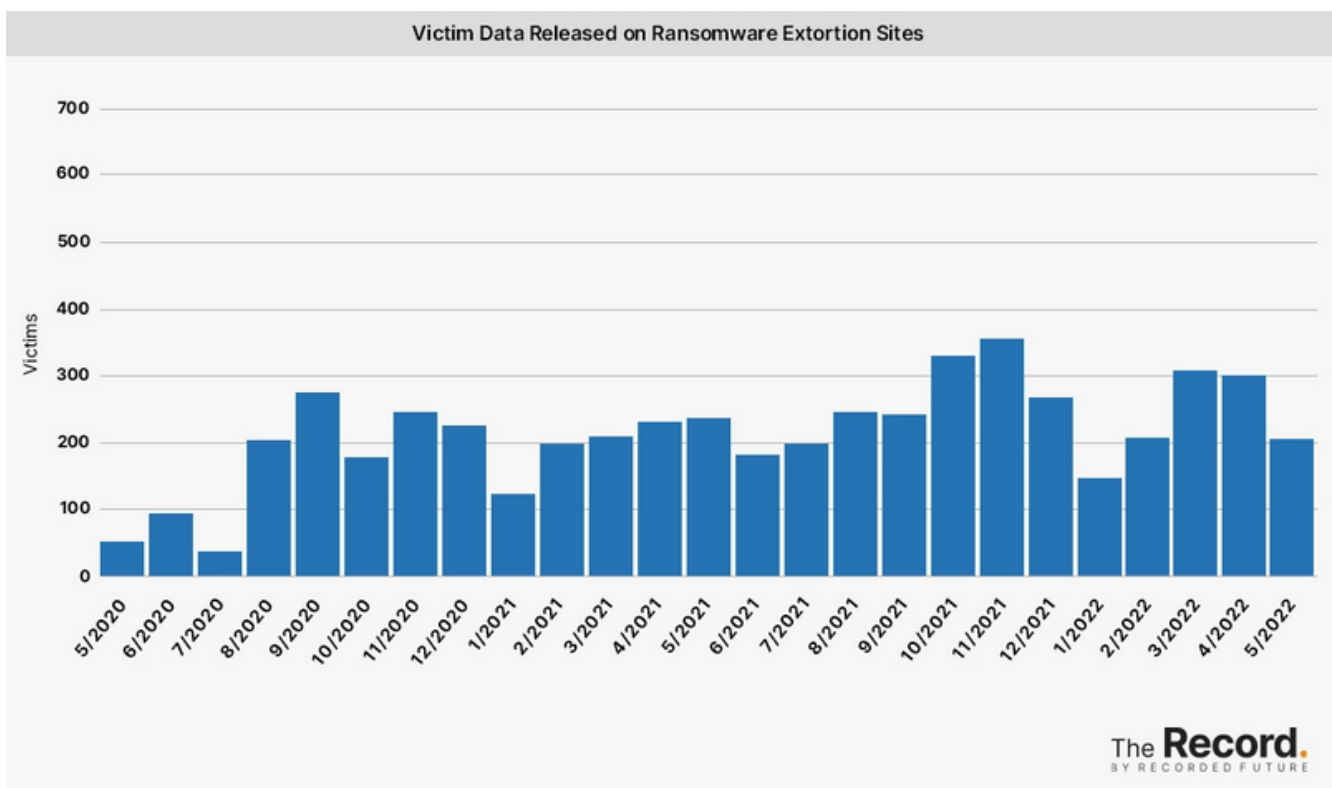


Now that you know you can buy ransomware off the Dark Web for a couple of bucks, you understand the severity of the cyber risks if you don't have the appropriate defense structures in place. Given that this threat is only expected to grow and evolve, staying aware of how cybercriminals acquire and release ransomware will help you avoid becoming a target on a day-to-day basis.

In 2021, ransomware is estimated to have...

- **victimized 37% of businesses**
- **been involved in 1 out of every 10 breaches, twice that of the year before**
- **cost victims approximately \$5.2B in Bitcoin, according to the US Treasury**
- **driven up the average payment by 82%**
- **included data leaks in 77% of successful breaches**

As 2022 projects a continuation of these trends, ransomware continues to be a prevalent attacker and organizations need a security posture that's prepared against the increasing likelihood of an attempted ransomware attack.



Source: therecord.media/ransomware-tracker-the-latest-figures/

QUICK CHECK-LIST:



Do you check the URL of a link before you click on it?



Have you downloaded ad blockers to your browser?



What backup storage do you have in place?



Do you know where to report suspicious messages?



viruses

data mining

keyloggers

camfecting

adware

worms

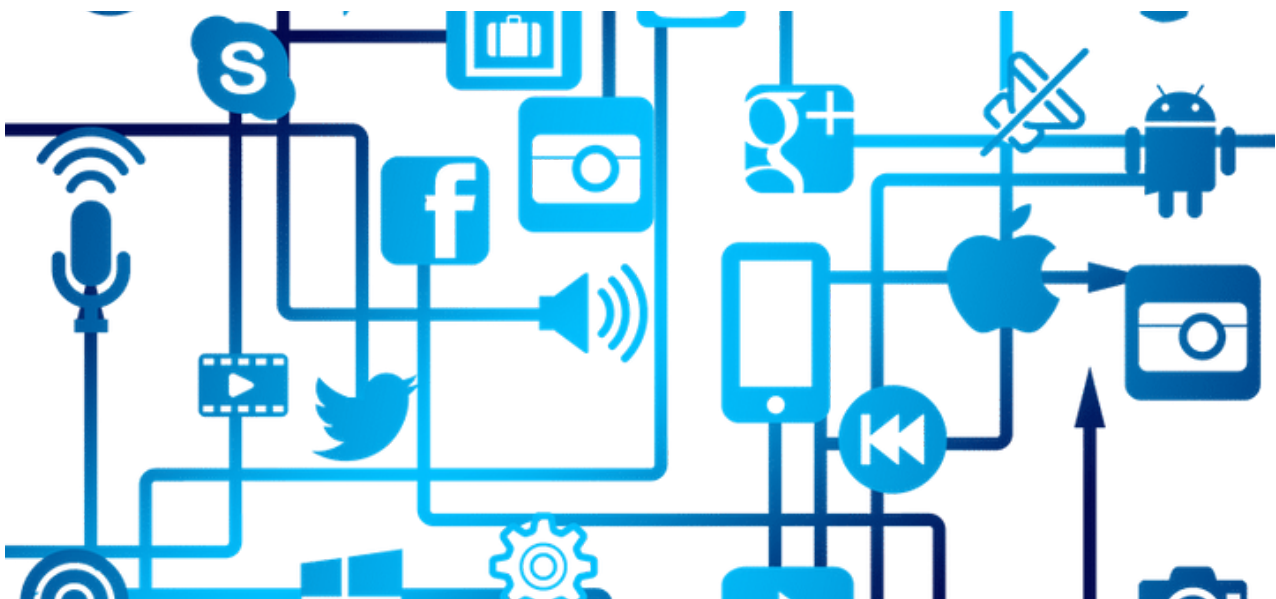
spoofed sites



How does ransomware work?

Ransomware is a type of malicious software, or malware, that blocks access to a system, device, or file until a certain amount is paid to the hacker. It is an illegal moneymaking scheme that can be installed through deceptive links in an email message, instant message or compromised website.

Ransomware works by encrypting files on the infected system (crypto ransomware), threatening to erase files (wiper ransomware), or blocking system access (locker ransomware) for the victim. The ransom amount and contact information for the cyber threat actor (CTA) is typically included in a ransom note that appears on the victim's screen after their files are locked or encrypted. Sometimes the CTA only includes contact information in the note and will negotiate the ransom amount once they are contacted. The demand is usually for cryptocurrency, such as Bitcoin, and can range from as little as several hundred dollars up to and exceeding one million dollars. It is not uncharacteristic to see multi-million-dollar ransom demands in today's threat landscape.



How is Ransomware Spread?

Ransomware is primarily delivered through some of the following means:

- Malicious attachments or links sent in an email
- Network intrusion through poorly-secured ports and services, such as Remote Desktop Protocol (RDP) (e.g. Phobos ransomware variant).
- Dropped by other malware infections (e.g. initial TrickBot infection leading to a Ryuk ransomware attack).
- Wormable and other forms of ransomware that exploit network vulnerabilities (e.g. the WannaCry ransomware variant).

It is a growing and expensive problem. While ransomware infections are not entirely preventable due to the effectiveness of well-crafted phishing emails and drive-by downloads from otherwise legitimate sites, organizations can significantly reduce the risk of ransomware by implementing cybersecurity policies and procedures as well as improving cybersecurity awareness and practices of all employees.



TOO LATE!

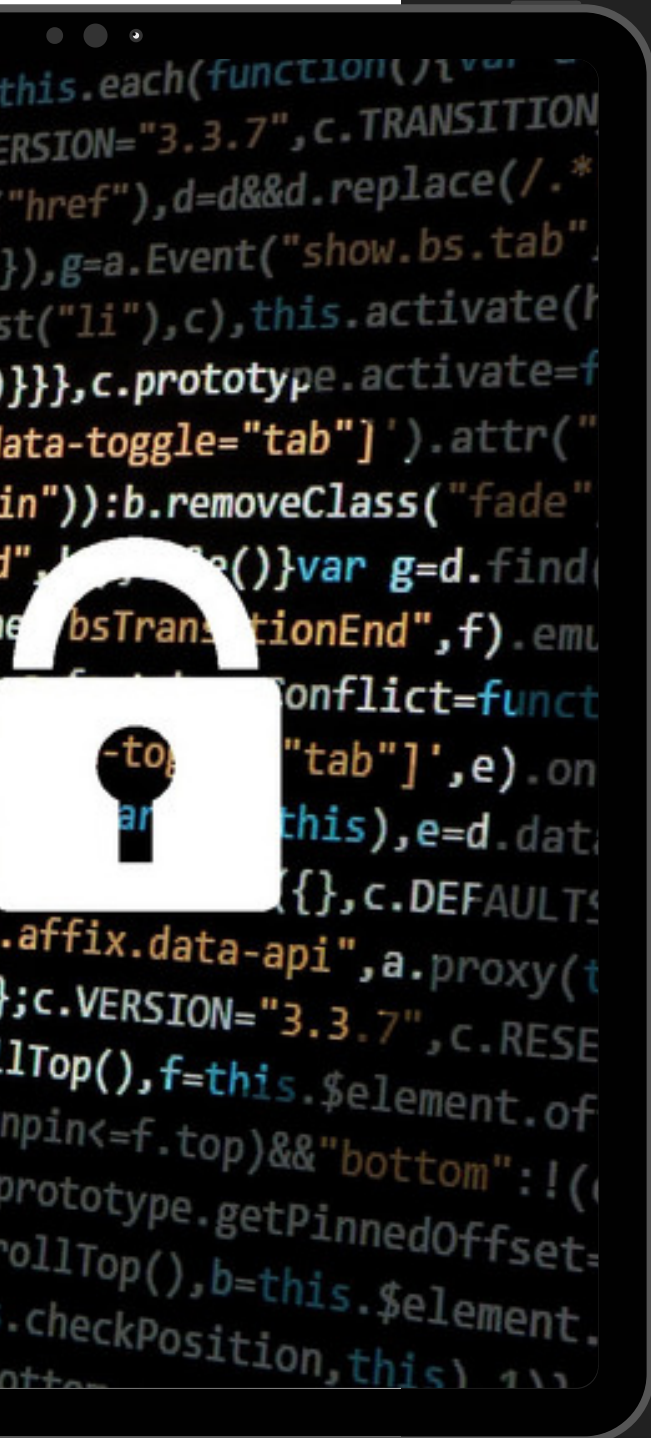
MY SYSTEM HAS

BEEN INFECTED!

WHAT TO DO IF YOU FIND RANSOMWARE ON YOUR DEVICE

If your organization is the victim of a ransomware infection, follow your organization's incident response procedures to report it. Alternatively, the Cybersecurity and Infrastructure Security Agency (CISA) provides a secure means for constituents and partners to report incidents, phishing attempts, malware and vulnerabilities. To submit a report, visit <https://us-cert.cisa.gov/report>.

After reporting that the breach has taken place to the applicable department set by your organization, there are some things you can do to respond. The most effective strategy to mitigate the risk of data loss resulting from a successful ransomware attack is having a comprehensive data backup process in place; however, backups must be stored off the network and tested regularly to ensure integrity.



It is up to all of us to help prevent ransomware from successfully infecting our systems. To increase the likelihood of preventing ransomware infections, organizations must implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. This program should include organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails. When employees can spot and avoid malicious emails, everyone plays a part in protecting the organization.

"Typically, fee demands are in bitcoin and can range from hundreds, to thousands, to hundreds of thousands of dollars."

WHAT DO
THESE
ATTACKS
LOOK LIKE
IN REAL
LIFE?



*security awareness
training matters*

HIGH PROFILE RANSOMWARE ATTACKS

a summary of the most famous ransomware attacks that have occurred recently:

01

Colonial Pipeline

One of the most recent high-profile ransomware attacks was on Colonial Pipeline, a major fuel pipeline that supplies the east coast. As a precaution, the company took the pipeline offline and said the attack didn't interfere with the systems operating the pipeline. The result of this shutdown could be increased gas prices along the East Coast, showing how impactful these attacks can be.

02

City of Baltimore

In May of 2019, Baltimore, MD, had its servers compromised by a ransomware attack. The attackers demanded payment in bitcoin (13 bitcoin, equal to roughly \$76K). The city was susceptible to a ransomware attack because of the lack of controls that it had in place. As a result of the attack, the city had to reallocate \$6M for additional information technology security and infrastructure.

03

Microsoft Exchange Attack

In January 2021, a series of attacks severely hurt Microsoft's exchange servers. This gave the attackers access to user emails, passwords, admin privileges and thus critical private information. It's estimated that the attack impacted as many as 250,000 servers.

Microsoft acted quickly and released a series of updates in March meant to patch the security exploit identified by the attackers. However, Microsoft found another round of ransomware later in March, which required yet another series of patches. This attack cost Microsoft millions in addition to the harm done to its brand.

04

Small Business Example

Larger companies get the majority of the headlines when they suffer ransomware attacks. That can make small businesses believe that they're less at risk than medium- or large-sized companies, however, that's simply not true. **Almost 50% of small businesses have experienced a ransomware attack.** That said, hackers often target small businesses due to the relative lack of internal controls and security procedures. Additionally, most small businesses are more likely to pay a ransom to get their systems up and running again. Remember, downtime is critical to a small business's bottom line.

Unfortunately, a ransomware attack can cost a small business as little as \$10K up to the hundreds of thousands. For example, a small start-up company in Europe sold high-end products online. Their IT security controls didn't go beyond what came with their systems — just the basics.

One day, an employee errantly opened a PDF that seemed to be from someone internal. The PDF downloaded the malicious software, and the company was locked out of all of its systems. They later received an email stating that they would get their data back if they paid 15K in cryptocurrency.

The hackers kept threatening the company by repeatedly sending email demands. The company ultimately didn't pay the hackers; however, they lost just as much if not more money than the ransom. Consider the cost of their systems being down and the cost of the workforce to increase their internal controls, and it's easy to calculate why.

WHERE RANSOMWARE IS HEADED NEXT

& how to protect your business

Ransomware is a form of malicious software that encrypts the target's files, making the target unable to access their data. A ransomware attacker will demand a fee to target the decryption key to re-access their software. Typically, fee demands are in bitcoin and can range from hundreds, to thousands, to hundreds of thousands of dollars.

Phishing

So, how do these attacks happen? The most common way a ransomware attack occurs is through phishing. Phishing is the process by which the attacker will include a malicious link in an email that seemingly comes from a trustworthy source. Once the link is clicked, the malicious software is downloaded to the target's computer.

In other ransomware attacks, the attacker may claim to be a law enforcement agency or the company's own IT department, saying it has to shut down and update the target's software. The attacker is then given full access by the unsuspecting victim and can begin the ransomware attack by encrypting the target's files.





Social Engineering

Social engineering is so popular that it's a part of almost all ransomware attacks today. It occurs when an attacker manipulates their target into clicking a malicious link, downloading malicious software, etc.

Social engineering often happens in conjunction with a phishing attack. Someone is pretending to be a trusted source (e.g., CEO or CFO of a company) and asks the target to upload software to their computer for their own safety. The target trusts that the email is from someone they know, and they comply with the directions resulting in the start of a ransomware attack.

Another form of a social engineering attack is baiting. For example, someone you know sends you a link to download music from a band you're interested in. Once the "music" is downloaded, the malicious software is immediately installed, thus leaving your system exposed.

“Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.”

- Bruce Schneier





How to Defend Your Business From Daily Threats

Cybersecurity is crucial to protecting your business from a ransomware attack. This approach includes the protection of your information, data, hardware, and software from cyber threats. Cybersecurity also involves data security, operational security, physical security, as well as your business' disaster recovery and business continuity plan.

With the steady increase of ransomware attacks in recent years, evolving crypto-related scams and the proliferation of dark web services, it only makes sense to find ways to protect your organization.



FOR YOUR CONSIDER- ATION:

How often do you undergo mandatory (or even optional) security awareness training courses? Have you had any education in how to stay safe online?

Aside from the old seminar from your school days about stranger danger and parents' lectures about staying anonymous online, many of competent professionals simply never got the chance to learn more about how they may be targeted by, for and through their online activity.

Cybersecurity threats can take many forms and target any individual within an organization. Although high-level security access would be ideal for the hacker, it's regardless effective to crack the passcodes for more accessible employees, who probably have lower levels of cybersecurity threat exposure and training. If they can steal or guess someone's credentials, regardless of whose, criminals can more easily breach the system's security and steal files off the network.

RISK MANAGEMENT



Since anyone can become a target, it's important for organizations to hold intensive cybersecurity awareness training programs that teaches staff, at ALL levels of the organization, how to recognize and respond to security threats as they arise in real time. Otherwise it's not a matter of if a breach happens, it's a matter of when.

Risk management is crucial in building a solid cyber defense structure. It's very unlikely that you'll *never* experience a digital threat in all your professional career. Therefore, it is critical to know a sensible plan for responding to and recuperating from cyberattacks.

Is your company giving cybersecurity their all? Talk to management about implementing awareness training!

Internal Processes and Procedures

Given the rise of ransomware attacks, having strong internal processes and procedures is now more critical than ever. Most cyber insurance carriers even ask for a supplemental ransomware application before they provide a quote for cyber insurance.

These applications ask specific questions about internal controls such as multi-factor authentication, off-site data backups, firewalls in place, encryption, etc. These internal controls limit a company's exposure to ransomware, thus making the cyber carrier more comfortable taking on the risk.

Risk Assessments

If you're wondering if your company could be susceptible to a ransomware attack, executing a cyber risk assessment of your systems will help give you the answer. A cyber risk assessment can help you identify and prioritize risks to your operation and risks resulting from the use of your information systems.

Furthermore, a cyber risk assessment will help your organization's leaders make critical, informed decisions about the security in place and the need (if any) to add additional measures. The evaluation can help you decide the impact that a ransomware attack would have on your organization and what current systems are most vulnerable to such an attack.



*When it comes to cybersecurity,
it takes a village.*

*It's NEVER too late to start
improving your ability to
combat potential breaches.*

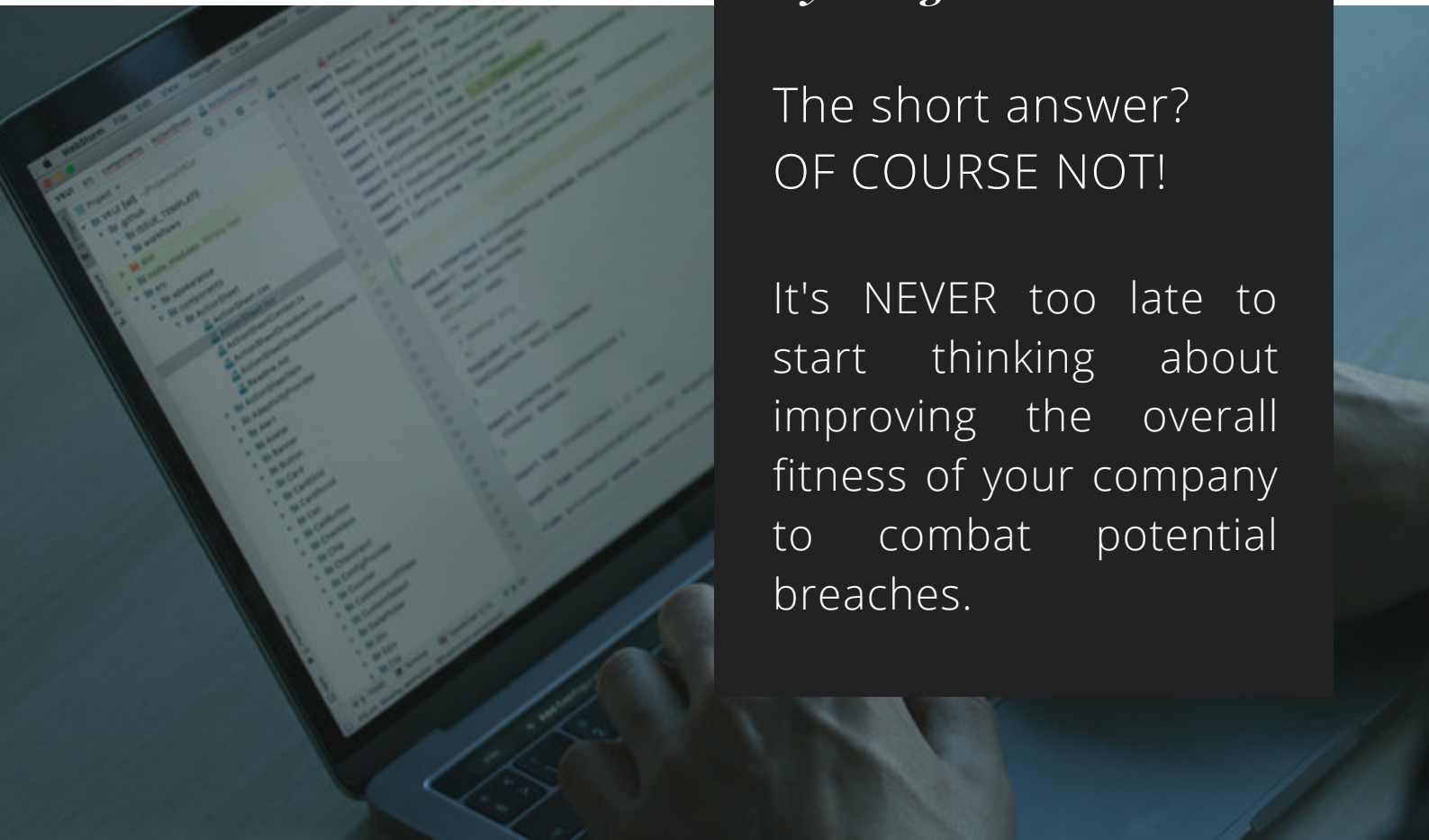




"HELP! Is it too late to start implementing strong cyber-awareness training within my organization?"

The short answer?
OF COURSE NOT!

It's NEVER too late to start thinking about improving the overall fitness of your company to combat potential breaches.



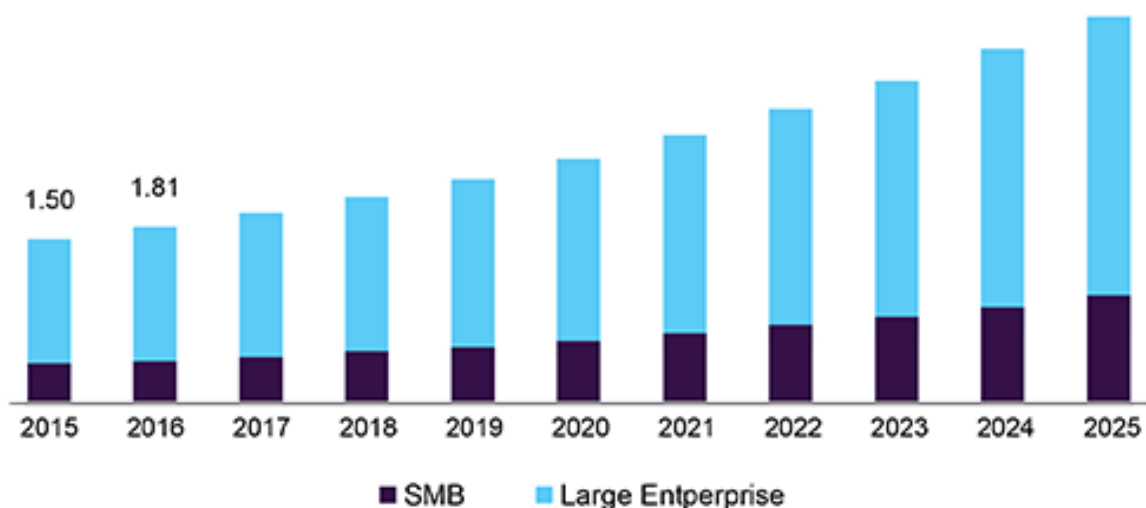
DOES CYBER INSURANCE COVER COMMON ATTACKS LIKE RANSOMWARE?

In a word, YES! Ransomware (most commonly seen as “extortion” on cyber liability insurance policies) is covered by preferred cyber liability carriers. In almost all cases, ransomware is covered up to the total limit of the cyber policy.

Finding the right policy for your individual business can be time-consuming, but it’s worth considering one that will effectively protect your company against a statistically-likely cyberattack. Consider ransomware protections as you’re researching the right policy for your business.



U.S. cyber insurance market size, by organization, 2015 - 2025 (USD Billion)



Source: www.grandviewresearch.com

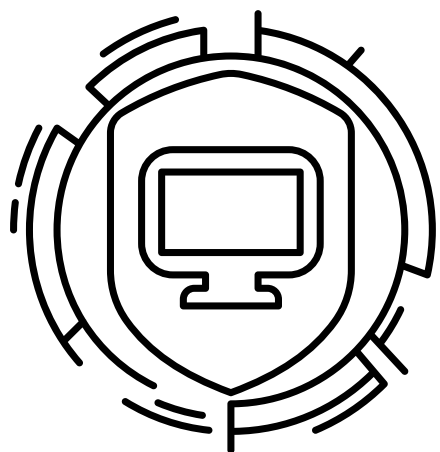
AWARENESS TRAINING: THE BEST DEFENSE

Have you ever gotten a phishing test email from your IT department? Tests like that coming out of the blue can be frustrating at times, but they're also extraordinarily necessary.

Did you know that 85% of data breaches result from human error?

Whether it's from failing to recognize a threat for what it is or a simple mistake at the end of a long week, one moment of oversight can end up costing the business tens of thousands of dollars just to recover from the resulting attack.

One of the greatest challenges in providing thorough cybersecurity awareness is the changing nature of cyber threats, which advance alongside technology developments. How can you keep on top of the biggest dangers to your business when they are so liable to change?

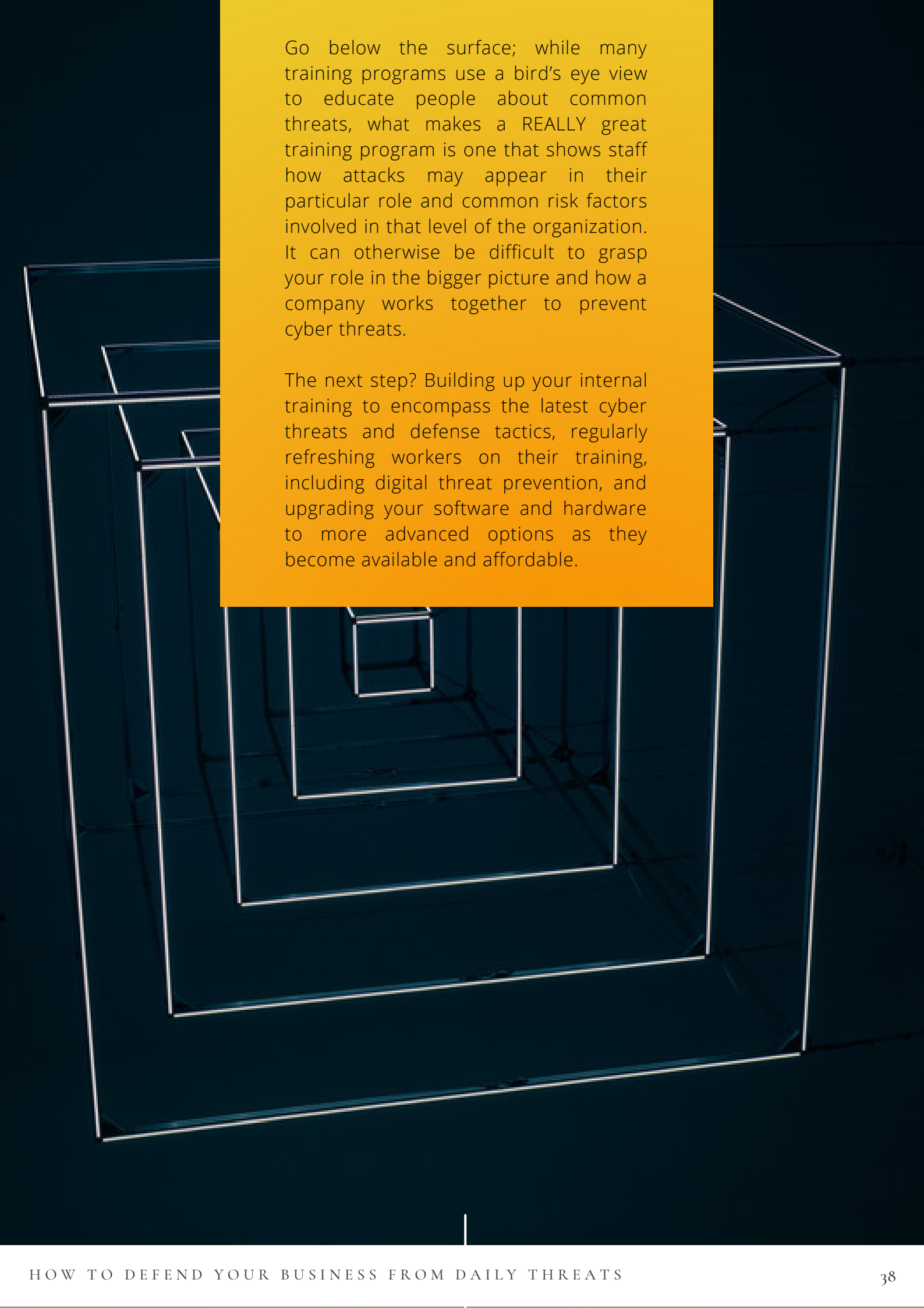


*Supporting
Company
Security
Awareness*

Some ideas to help employees grasp the crucial messages of their cybersecurity training:

- Hold regular training and refreshers to keep everyone apprised of the latest threats
- Find creative ways to bring the point home and keep employees engaged during training
- Include security awareness training in the company onboarding process, to reduce the risk of liability with new hires and streamline the process for all future staff
- Reward good behavior and, when mistakes occur, educate instead of punish





Go below the surface; while many training programs use a bird's eye view to educate people about common threats, what makes a REALLY great training program is one that shows staff how attacks may appear in their particular role and common risk factors involved in that level of the organization. It can otherwise be difficult to grasp your role in the bigger picture and how a company works together to prevent cyber threats.

The next step? Building up your internal training to encompass the latest cyber threats and defense tactics, regularly refreshing workers on their training, including digital threat prevention, and upgrading your software and hardware to more advanced options as they become available and affordable.

HOW TO BUILD BETTER INTERNAL TRAINING

When creating, expanding or updating your cybersecurity awareness program, what are important aspects to include?

What to do when someone encounters a threat, including any reporting protocol that must be followed

The most up-to-date tactics that cybercriminals use in social engineering attacks

How to identify safe sites and software

An overview of the threats most likely to target your business, based on its industry or location as well as other factors

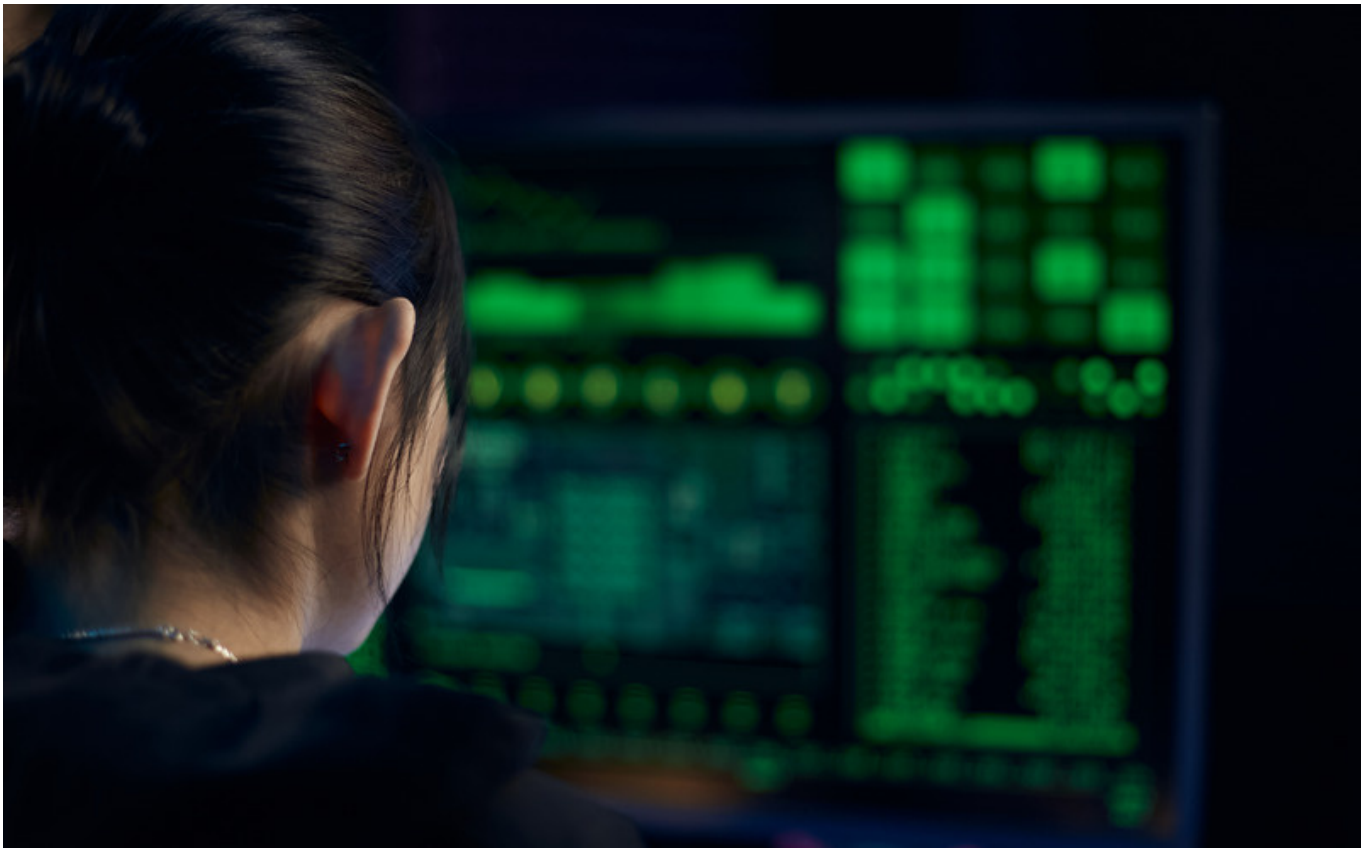
How to set up multi-factor authentication on their accounts

Education on how and why to update software regularly

Password security such as using a variety of alphanumerical characters, password managers, changing them routinely and generating different passwords for different accounts

The dangers of trusting unknown people and/or devices

BUSINESS MADE SAFER



TAKEAWAYS FROM DAILY DEFENSE TIPS & SECURITY AWARENESS TRAININGS

Staying aware of the latest in cybersecurity news will also tell you when there are new technologies or tactics that you, and your company as a whole, should employ for a more up-to-date security posture. A strong cybersecurity awareness training program prepares employees for the inevitability of attempted (and successful) breaches, with particular consideration on how their role plays into the greater picture of the company's overall defense posture. When it comes to cybersecurity, it takes a village.



"Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information."

- Kevin Mitnick

*Confidence in your
cybersecurity experts,
no matter what dream
you follow next.*



"It is a fairly open secret that almost all systems can be hacked, somehow. It is a less spoken of secret that such hacking has actually gone quite mainstream."

- Dan Kaminsky

```
header0_initialPadding = 'px';  
if ($(window).scrollTop() > header1_initialDistance) {  
  if (parseInt(header1.css('padding-top'), 10) >= header1_initialPadding + $(window).scrollTop() - header1_initialDistance) {  
    header1.css('padding-top', '' + $(window).scrollTop() - header1_initialDistance + 'px');  
  }  
} else {  
  header1.css('padding-top', '' + header1_initialPadding + 'px');  
}  
  
if ($(window).scrollTop() > header2_initialDistance) {  
  if (parseInt(header2.css('padding-top'), 10) >= header2_initialPadding + $(window).scrollTop() - header2_initialDistance) {  
    header2.css('padding-top', '' + $(window).scrollTop() - header2_initialDistance + 'px');  
  }  
} else {  
  header2.css('padding-top', '' + header2_initialPadding + 'px');  
}
```

Get Our Monthly Cybersecurity Newsletter

CONTINUE TO GET MORE FREQUENT UPDATES



WWW.RESTECH.SOLUTIONS

Bringing you the cybersecurity news YOU need to stay up to date on the latest tricks and trends coming out of the dark web, as well as what security experts are developing to fight them.

SIGN UP NOW!

SIGN UP FOR OUR MONTHLY CYBERSECURITY NEWSLETTER

REVIEWS!

Elle Mobbs



Owner of RTW Specialists

★★★★★

Understands our Needs

ResTech took the time to analyze our needs and helped us obtain the necessary tools to grow our business and they understood our needs and goals.

Dr. Sandra Scurria



Houston, TX

★★★★★

Prompt & Reliable

ResTech provides a very prompt response to my requests for help. I can rely on ResTech to solve my issues because they are persistent and will work with me until they solve the problem.

Michael Williams



Houston, TX

★★★★★

Easy to Work With

ResTech has been easy to work with as they are very responsive. They will ensure any issue gets addressed and they don't make me wait for support. I have been very satisfied with ResTech Solutions!

David Sawicki



Owner of AB7 Property Management

★★★★★

Quickly Identifies Solutions

When we call or email, ResTech is readily available to provide the support we need. They can quickly identify solutions and provide me with alternative options as well. I recommend ResTech without hesitation!

CYBERSECURITY YOU CAN TRUST!



We believe in providing YOU the best-in-class security suite to keep you cyber-secure in the face of the ever-changing threat landscape.

Call us today at **713-936-6855** and let us help you wrap a security blanket around your business.