Cybersecurity

TRAINING GUIDE

for U.S. Businesses

With *Recruiting Roadmap* Addendum

Protect your business from pervasive cyber threats

Table of Contents

Cybersecurity Training Guide for U.S. Businesses

Introduction

Adopting and implementing stronger cybersecurity protections is now a strategic business imperative.

*"**Ransomware activity jumped an astounding sevenfold** in the second half of 2020 compared with the first six months." FortiGuard Labs Threat Report: Disruption Key Threat Trend in 2020*

2020 and much of 2021 has been a trial for most organizations in the United States, especially regarding cybersecurity. As a result, most companies are keenly aware of the importance of data and systems protection to their business continuity, growth and profitability.

The daily barrage of reports of cyber intrusions into government systems and ransomware demands to unlock hacker-encrypted company data in private business information and operational systems has been hard to ignore.

A recent global survey by cybersecurity company Sophos found that only 65% of encrypted data was restored after the ransom was paid and that the average bill for rectifying a ransomware attack - considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. - was $1.85 million.

Company executives are increasingly aware of the role cybersecurity plays in not just preventing data loss and expensive ransom demands, but in avoiding costly customer lawsuits and lengthy business disruptions that can potentially cripple their operations.

As a result, corporate leaders are increasingly elevating the importance of cybersecurity to their companies. Looking ahead, it is critical to continue elevating cybersecurity as a strategic business issue and develop more threat-sharing partnerships between industries, business leaders, regulators, and policymakers.

This comprehensive and professionally researched Cybersecurity Training Guide will help you create or upgrade your cybersecurity system and processes by helping you to:

- Better understand security in the COVID and post-COVID eras,
- Build effective security plans and budgets, and
- Understand and defend against different types of cyber threats that are increasing in both scope and frequency and implement practical solutions to the same – including educating employees whose personal smartphone and home device practices have greater business impacts now that remote work from home appears here to stay.

Let's get started!

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 1

Cybersecurity – An Overview

Cybersecurity Definition

Cybersecurity is the process of protecting systems, devices, networks, and data from any type of unauthorized access or attack. Cyber-attacks typically try to gain access to sensitive information and alter, disrupt, destroy, control or steal that information for malicious or criminal intent.

A survey by cybersecurity company Sophos found that **51% of respondent businesses in the U.S**. were hit by ransomware attacks in the past year. Simply paying a ransom is no guarantee a company's encrypted data will be successfully restored and the company able to resume operations since nearly half of businesses that regain access get back tainted data.

Data encryption is giving way to extortion-style attacks where instead of encrypting files the attackers steal and threaten to publish company data unless their ransom demand is paid. This entails less effort for them as no encryption or decryption is needed. By the end of 2020, data theft as additional leverage in ransomware campaigns was used in a majority of attacks.

These attacks are of increasing concern to businesses. As more information and data moves online, everything from emails and credit cards to energy grids, navigation systems, medical records and intellectual property are susceptible to digital attacks.

a. Common Types of Threats

Cyber-attacks can vary in size and scope, but some common types of threats include:

- **Phishing**

This usually takes the form of emails that appear as though they are from a reputable and legitimate source. These fraudulent communications aim to steal sensitive details, such as login information or credit card numbers.

- **Malware**

Malware is malicious software that has been designed to gain unauthorized access or disrupt a computer. It typically breaches a network if a user clicks on a dangerous link, email attachment, or download. Malware can take many forms, including viruses, Trojans, worms, spyware, and ransomware.

- **Man-in-the-Middle Attack**

This type of attack involves a cybercriminal intercepting a communication between two parties. The criminal eavesdrops on the conversation and impersonates one or both parties to control information, steal data or redirect financial payments.

- **Denial-of-Service Attack**

In this attack, cybercriminals overwhelm and exhaust networks and servers with traffic to shut down or disrupt the availability of services. The resources are then unavailable or inaccessible for legitimate users.

- **SQL Injection**

An SQL, or Structured Language Query, injection happens when malicious SQL code is inserted into an application's database via an SQL statement, allowing attackers to view sensitive data.

The purpose of cybersecurity is to defend against these common threats by building systems and developing tactics to protect data. Cybersecurity is also sometimes referred to as information technology security, though it also extends to operational technologies like industrial control and SCADA systems that impact physical processes.

b. Types of Cybersecurity

There are five main types of cybersecurity: critical infrastructure security, mobile and application security, network security, cloud security, and internet-of-things (IoT) security.

- **Critical Infrastructure Security**

Critical infrastructure includes systems and networks that society relies on, such as electricity grids, critical manufacturers, traffic lights, water purification, and hospitals. Though these are physical infrastructures, they rely on cyber systems. Governments work with the owners and operators of critical infrastructure to better secure them from potential cyber-attacks.

- **Network Security**

This type of cybersecurity protects internal networks from unauthorized access. Different tools, policies, and procedures are used in attempting to ensure networks are not exploited. Common tools include firewalls, antivirus and antimalware programs, and virtual private networks.

- **Mobile and Application Security**

As users store more personal data on smartphones, tablets, laptops, and other devices, mobile security is an increasingly important concern. If a device is lost or stolen, there are tools that can lock the use of a mobile device or require multi-factor passwords before they can be accessed.

Within mobile security is application security, which is the process of finding, preventing, and fixing any vulnerabilities in apps. Cybersecurity professionals work to make apps more secure so there is less risk of unauthorized access to data and devices. Application security starts during the design and development stages and continues after apps are deployed.

- **Cloud Security**

This type of cybersecurity protects data and applications that are stored on cloud-based systems. The major threats to cloud security include data being exposed, unauthorized users accessing data, and malicious attacks to infect or destroy cloud infrastructure. Common defenses in cloud security include encryption, firewalls, and virtual private networks.

- **Internet-of-things Security**

The internet-of-things (IoT) refers to a variety of systems connected to the internet, such as business information and operating systems, Wi-Fi routers, and security cameras. Many IoT devices have weak encryption and unpatched vulnerabilities, which means they can be easily exploited. The increasing number of IoT devices makes this a high priority area in cybersecurity, especially for the Industrial Internet-of-Things (IIoT).

c. Why Is Cybersecurity Important?

Cybersecurity is important because so much of our sensitive information - including companies' intellectual property and information systems - are vulnerable to attack and need to be properly protected.

Cyber-attacks can happen to any size organization, big or small. In addition to attacks on businesses, there have been many incidences of governmental organizations being breached and citizens losing access to essential services. On both an individual and organizational level, cybercrime victims have faced identity theft, blackmail and extortion.

Cyber-attacks are one of the world's fastest growing crimes. It is expected that cybercrime damages could be costing the world $6 trillion annually.

Cyber criminals are becoming more innovative and brazen in their tactics, making cybersecurity critically important.

d. Benefits of Cybersecurity

There are many benefits and advantages to effective cybersecurity. Some of the key benefits are that it protects data against unauthorized access, improves business performance and helps build confidence in customers who are also quite aware of the escalation in cybercrime that puts their private data at risk.

- **Protects against cyber-attacks.**

Cybersecurity tools and processes assess vulnerabilities and help prevent threats from infiltrating systems. This keeps sensitive data more secure and attempts to ensure that only authorized users can access information.

- **Helps save time and money.**

Viruses can slow down computers and cause interruptions in business operations. If a significant breach occurs, it can be costly to bring in outside services and experts to deal with the consequences. In the long run, cybersecurity measures will save businesses time and money - especially in comparison with multimillion dollar ransom payments.

- **Improves customer confidence.**

A robust cybersecurity strategy and implementation will inspire confidence in customers. Many businesses gather information from their customers, so customers need to feel that their data is in safe hands.

- **Speeds recovery from a data breach**

In the event there is a cyber-attack, having the right policies and recovery plans in place will allow the company to quickly recover and resume business operations.

e. Using Automation in Cybersecurity:

Automation has become an integral component in helping keep companies protected from the growing number and sophistication of cyberthreats. Using artificial intelligence (AI) and machine learning in areas with high-volume data streams can help improve cybersecurity in three main categories:

- **Threat detection:** AI platforms can analyze massive amounts of data and recognize known threats, as well as predict novel threats.
- **Threat response:** AI platforms also create and automatically enact security protections.
- **Human augmentation:** Security pros are often overloaded with alerts and repetitive tasks. AI can help eliminate alert fatigue by automatically triaging low-risk alarms and automating big data analysis and other repetitive tasks, freeing humans for more sophisticated tasks.
- Other benefits of automation in cybersecurity include attack classification, malware classification, traffic analysis, compliance analysis and more.

f. Top Cybersecurity Challenges

Cybersecurity is continually challenged by hackers, data loss, privacy, risk management and changing cybersecurity strategies. The number of cyberattacks is not expected to decrease any time soon. Moreover, increased entry points for attacks - such as with the arrival of the internet of things (IoT) and **dramatic increase in remote work from home** due to the coronavirus pandemic - increase companies' attack surfaces and their need to secure networks and devices.

One of the most problematic elements of cybersecurity is the evolving nature of security risks. As new technologies emerge, and as technology is used in new or different ways, new attack avenues are developed. Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging. Issues include ensuring all elements of cybersecurity are continually updated to protect against potential vulnerabilities. This can be especially difficult for smaller organizations without the staff or in-house resources.

Additionally, organizations can gather a lot of potential data on individuals who use one or more of their services. With more data being collected, the likelihood of a cybercriminal who wants to steal personally identifiable information (PII) is another concern. For example, organizations that stores PII in the cloud may be subject to ransomware attacks that require them to include prevention of cloud breaches in their cybersecurity efforts.

Cybersecurity programs should also address end-user education, as employees may accidently bring viruses into the workplace on their laptops or mobile devices. Regular security awareness training will help employees do their part in keeping their company safe from cyberthreats.

Another challenge to cybersecurity includes a shortage of qualified cybersecurity personnel. As the amount of data collected and used by businesses grows, the need for cybersecurity staff to analyze, manage and respond to incidents also increases. (ISC)2 estimated the workplace gap between needed cybersecurity jobs and security professionals at 3.1 million.

Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats while lesser-known threats were left undefended, is no longer sufficient. To keep up with changing security risks, a more proactive and adaptive approach is necessary.

Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

The federal Cybersecurity and Infrastructure Security Agency (CISA) lists the following as today's major cyber threats:

You can watch the CISA webinar describing these cyber threats in detail here.

Sophos' "Active Adversary Playbook 2021" findings showed the median attacker dwell time in 2020 and early 2021 before detection was 11 days – or 264 hours – with the longest undetected intrusion lasting 15 months. Ransomware featured in 81% of incidents.

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 2

Latest Cybersecurity Trends

In the past year-plus, COVID-19 has had a larger impact on work habits and security environments than any other health emergency in memory. Combined with technological advances such as 5G, this has led to several trends expected this year and next.

Here are the top cybersecurity trends:

a. Increasing Attacks on Remote Infrastructure.

Because of the pandemic, there was an enormous increase in the number of workers moving from centralized locations to home offices. A recent PriceWaterhouseCoopers (PWC) survey found that 78% of CEOs believe that a distributed (work from home) workforce is here to stay.

As a result, organizations must rethink how they can best organize themselves in these uncertain times, remain secure and survive this indefinite period of remote work and virtual interactions.

Many companies are struggling to adapt their security strategy to accommodate this new normal. With remote work an ongoing reality, there's been a rush to adopt and integrate new tools and cloud platforms to facilitate collaboration and maintain productivity.

This, in turn, has led to increased use of technologies facilitating remote work, such as email, VPN and remote desktop (RDP). This means that relying solely on a corporate firewall is no longer a sound security strategy.

In many cases, workers began working remotely so quickly that organizations did not have enough time to fully consider security implications. This created an increased attack landscape in which criminals understand security weak points and how to capitalize on them, particularly with VPN. Sadly, we have seen several compromises already and expect to see this continue. Suffice to say, companies must focus on securing both their VPN and RDP infrastructures.

b. Smart Devices Evolving from Connected to Autonomous.

Smart cities, smart manufacturing, smart transport and logistics will continue to become more autonomous. Smart devices used for automation in manufacturing plants, transport, and logistics will become more autonomous, with more built-in intelligence and reduced full-time connections.

This will have an impact on latency, availability of connections and security.

The latency issue is a product of having to talk to centralized cloud services, which takes more time than is ideal for real-time systems to react to things occurring in the physical world.

Likewise, a loss of connectivity for any number of reasons (power outage, cloud down, cyberattack) can impact smart devices that are not autonomous. And the more you are connected and interact with external services, the higher risk of security exposure to attack.

As such, we will see more smart systems that run by themselves using connections for remote monitoring. Intelligence will be provided by multi-access edge computing (MEC) and edge cloud services and 5G's blazing speed will be a critical driver for smart collaboration between systems.

c. The Internet as One Large Interconnected Service Factory.

APIs for web applications have allowed organizations to take some services and place them in different interconnected clouds. This is the beginning of a full mesh of interconnected services from the edge to central clouds, effectively creating a full meshed hierarchy.

The risk is that if one component fails, then the whole system is impacted. Centralization in major cloud providers such as Amazon Web Services (AWS), Amazon Azure and Google Cloud increases the probability for large scale outages. Expect to see more in the coming years.

We will see larger impacts due to centralization, including widespread outages and collateral damage. Most users of common intelligent devices don't understand what they're connected to.

So when AWS goes down and IoT devices stop working, it can be problematic. We have come to rely on smart systems without considering the importance of secure and reliable connections.

d. More Advanced Non-Nation State Users Will Attempt to Influence and Disrupt.

Ordinary users are now learning the tactics, techniques and procedures (TTPs) being used by Advanced Persistent Threat (APT) groups and other cybercriminal organizations. More cyber operations by domestic cybercriminals are likely to influence and disrupt business processes. And because of their easy access to social media, they may have a significant impact.

e. Internet Providers will Need More Bandwidth for "Gray Noise".

Scanning by white, gray, and black hats, as well as DDoS attacks, consumes internet bandwidth. As such, every internet exchange, transit provider and ISP will have to take this traffic into account when sizing their networks.

Increased gray noise makes it more time consuming and expensive to determine good traffic from bad. In the end, the costs for this will be passed on to businesses and consumers.

f. Expect More Bad Bot Problems.

In 2020, we saw PS5/XBOX Series X|S scalping campaigns impact consumers. Now, individuals are using sniping bots to counter scalpers on marketplaces. And it is not just malicious actors or hackers that are building scripts to buy something faster.

Ordinary people are buying tools or building tools learned via YouTube videos to do this. If you do not have a bot, you are now at a disadvantage of buying coveted products. Businesses will need advanced bot mitigation to better protect themselves and their brands from individuals using bots that limit availability to potential customers.

g. Ransomware Will Continue to Rule the Land.

The total number of ransomware attacks quintupled globally over the last two years and is expected to rise 20 to 40 percent in 2021.

In response, the federal Cybersecurity and Infrastructure Security Agency (CISA) has issued no-cost resources to help businesses keep their organizations secure. Some of their messaging is summarized in the following graphic:

Expect even more emails with enticements to click on nefarious links. These phishing schemes may use topical issues like early access to COVID-19 vaccinations or other subjects with a strong emotional pull. As a result, expect even more ransomware payloads delivered via phishing emails.

Perhaps nothing is more emblematic of the pervasiveness and persistence of ransomware as the emergence of Ransomware-as-a-Service (RaaS). RaaS brings the lucrative business model of ransomware to even the most tech-deficient of aspiring cybercriminal entrepreneurs and threatens to turn ransomware into a commodity that will assure its endurance for the foreseeable future.

Here are two other entries from CISA about this dangerous phenomenon to end this chapter:

Trend: Ransomware-as-a-Service (RaaS) Model

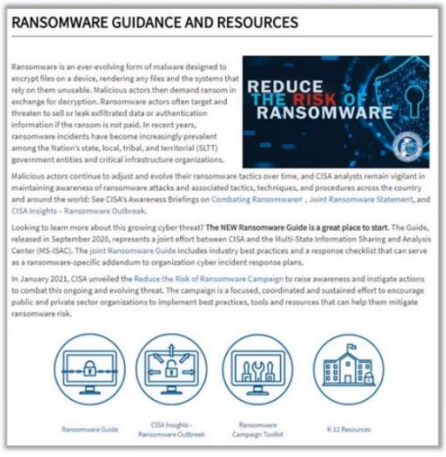
- Ransomware families selling RaaS to other cybercriminals.
- Popularity increases ➔ Barriers to entry drop, becomes scalable, more efficient.
- Enables relatively unskilled bad actors to access complex tools and the environment from which to run their campaigns.
- The "commoditization" of the ransomware threat: Entrepreneurial Operators, including NetWalker, Nefilim, and Sodinokibi/Revil all provide access to partners in pre-agreed profit-sharing arrangements.
- Increased investment in many of the platforms themselves, upgrading their core ransomware systems to stay ahead of the good guys and evade detection.

CISA resources for ransomware are summarized below:

CISA Ransomware Resources

CISA.gov/ransomware

- **Ransomware Guide**
- **CISA INSIGHTS: Ransomware Outbreak**
- **NEW! Toolkit, fact sheet, and images**
- **Alerts and Statements**
  - Rising Ransomware Threats to OT Assets Face Sheet
  - US-CERT activity alerts on ransomware threats
  - Joint statements on ransomware with our partners
- **Guides and Services**
  - Cyber Hygiene Services
  - TTX Exercises
- **Factsheets and Infographics**
  - Protect Your Center From Ransomware poster
  - Ransomware: What It Is and What To Do About It
- **Training and Webinars**
  - Trends and Predictions in Ransomware
  - CDM Training
  - Incident Response Training Series
  - Combating Ransomware Webinar



[Click Here to Find Funding for Your Cybersecurity Needs – Up to $33K Per Employee]

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 3

A Guide to Hacking and How to Avoid It

a. What is Hacking?

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit its security and gain access to personal or business data. An example of computer hacking is using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful business. It is not enough to have isolated computer systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking.

System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

b. Types of Hackers and Hacks

There are typically four key drivers that lead bad actors to hack websites or systems:

(1) Financial gain through the theft of credit card details or by defrauding financial services,
(2) Corporate espionage,
(3) To gain notoriety or respect for their hacking talents, and
(4) State-sponsored hacking that aims to steal business information and national intelligence.

In addition, there are politically motivated hackers - or hacktivists - aiming to raise public attention by leaking sensitive information (e.g., Anonymous, LulzSec and WikiLeaks).

A few of the most common types of hackers carrying out these activities include:

- **Black Hat Hackers**

Black hat hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage or as part of a nation-state hacking campaign.

These individuals' actions can inflict serious damage on both computer users and their employers. They can steal sensitive personal information, compromise computer and financial systems, and alter or take down the functionality of websites and critical networks.

- **White Hat Hackers**

White hat hackers can be seen as "good guys" attempting to prevent the success of black hat hackers via proactive hacking for organizations that employ them. They use their technical skills to break into systems to assess and test the level of network security (aka ethical hacking). This helps expose vulnerabilities in systems before black hat hackers can detect and exploit them.

The techniques white hat hackers use may be identical to those of black hat hackers, but they are hired by organizations to test and discover potential holes in their security defenses.

- **Gray Hat Hackers**

Gray hat hackers sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. Their actions are typically carried out for the common good. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly. This alerts organizations and the public generally to the existence of the vulnerability.

c. Devices Most Vulnerable to Hacking

- **Smart Devices**

Smart devices, such as smartphones, are lucrative targets for hackers. Android devices have a more open-source and inconsistent software development process than Apple devices, which puts them at greater risk of data theft or corruption. Hackers are increasingly targeting the millions of smart devices connected to the Internet of Things (IoT).

- **Webcams**

Webcams built into computers are a common hacking target, mainly because hacking them is a simple process. Hackers typically gain access to a computer using a Remote Access Trojan (RAT) in rootkit malware, which allows them to not only spy on users but also read their messages, see their browsing activity, take screenshots, and hijack their webcam.

- **Routers**

Hacking routers enables an attacker to gain access to data sent and received across them and networks that are accessed on them. Hackers can also hijack a router to carry out wider malicious acts such as distributed denial-of-service (DDoS) attacks, Domain Name System (DNS) spoofing, or crypto mining.

- **Email**

Email is one of the most common targets of cyberattacks. It is used to spread malware and ransomware and as a tactic for phishing attacks, which enable attackers to target victims with malicious attachments or links.

- **Jailbroken Mobile Phones**

Jailbreaking a phone means removing restrictions imposed on its operating system to enable the user to install applications or other software not available through its official app store. Aside from being a violation of the end-user's license agreement with the phone developer, jailbreaking exposes many vulnerabilities. Hackers can target jailbroken phones, which allows them to steal any data on the device but also extend their attack to connected networks and systems.

d. How Hacking Works

Hacking techniques are ever evolving and it's important to keep up with new threats. Hackers are usually after two things from your business: data or money. Usually they are motivated by both, as uncovering a wealth of data can help them to cash in.

Just how do these hackers find vulnerabilities in systems, exploit them, and gain personally?

Three major routes reign supreme:

- **Social engineering:** The simplest way to hack an account or system? Just ask the user for their password! This may take the form of phishing or spam phone calls, so be careful who you give your credentials to. Once a hacker has your password, they can easily grab your credit and debit card information, social security number, and other information you want to keep confidential.

- **Programming-Based Hacking:** This is more advanced than social engineering, as programming-based hacking requires the hacker to find vulnerabilities in a system and take over all administrative privileges.

- **Physical Access:** Possibly the easiest way to hack into a computer or system is to have physical access to it for a long time. Because of this, physical security of business facilities is an integral component of a comprehensive cybersecurity regimen.

Other common ways to hack are:

- **Malware-Injecting Devices:** Cybercriminals can use hardware to sneak malware onto your computer. You may have heard of infected USB sticks that can give hackers remote access to your device as soon as they are plugged into your computer.

  All it takes is for one person to give you a malware-ridden USB stick, and by simply plugging it into your computer, you are infected. Clever hackers are using cords now to inject malware - like USB cables and mouse cords - so it is crucial to always think before plugging anything into a work device or personal device with access to work-related data.

- **Missing Security Patches:** Security tools become outdated as the hacking landscape advances and require frequent updates to protect against new threats. However, some users ignore update notifications or security patches, leaving themselves vulnerable.

- **Distributed Denial-of-Service (DDoS):** This hacking technique is aimed at taking down a website so that a user cannot access it or deliver their service. DDoS attacks work by inundating the target's server with large influxes of traffic that are so high and frequent that it overloads the server with more requests than it can handle. Ultimately, the server crashes and the website goes down with it.

  Larger businesses can get hit by DDoS attacks synchronized on more than one server or website, potentially taking down numerous online assets. A cloud protection service or DDoS mitigation service can help protect the business from a site takedown.

e. Why Hacking is Bad

Hacking can be used for good or evil. Starting with the bad, non-ethical hackers can:

- Steal credit card information, personal information, login credentials, and more
- Attack national security of other countries
- Inject malware into computers.
- Modify or destroy data.

Ethical hackers, on the other hand, can use hacking for:

- Hacktivism, meaning political or social causes.
- Improving security of websites or apps.

Considering the ransomware and Trojan attacks currently favored by criminal hackers, the question now is: how can I protect my business from hacking?

f. Tips to Stay Safe from Hacking.

The U.S. National Security Agency has released a list of evasion and exfiltration techniques the Russian intelligence agency GRU has used to help IT managers identify - and stop - attacks by this dominant hacking group. The lack of sophistication by GRU means fairly basic measures - like multifactor authentication, timeout locks, and temporary disabling of accounts after incorrect passwords are entered - can effectively block their brute force attacks.

Following are additional measures companies can employ to deter or prevent such attacks.

- **Implement network segmentation.**

Spreading your data across smaller subnetworks reduces your exposure during an attack. This can help contain infections to only a few endpoints instead of your entire infrastructure.

- **Enforce the principle of least privilege (PoLP).**

By only giving users the access level they need to do their jobs and nothing more you can minimize the potential damage from ransomware attacks.

- **Backup all your data**.

This goes for all the endpoints on your network and network shares too. If your data is archived, you can always wipe an infected system and restore it from a backup.

- **Educate end users on how to spot mail spam**.

Users should be wary of unsolicited emails and attachments from unknown senders. Train end users to inquire further if suspicious emails appear to be from a trusted source and to check the "from" address in the email to confirm its legitimacy before opening it or clicking a link in it.

- **Educate staff on creating strong passwords.**

And implement some form of multi-factor authentication (MFA)—two-factor authentication at a bare minimum.

- **Patch and update your software**.

Routinely and consistently.

- **Implement a Zero-Trust architecture.**

Many networks are based on implicit trust where whoever gains access to a corporate IT network is assumed to be trustworthy and deserving of access to data, systems and applications across the network. Traditional reliance on virtual private networks (VPNs) has proven inadequate as VPNs provide virtually no inspection and verification of the legitimacy of the traffic passing through it. This makes it only as secure as the devices and networks from which it connects.

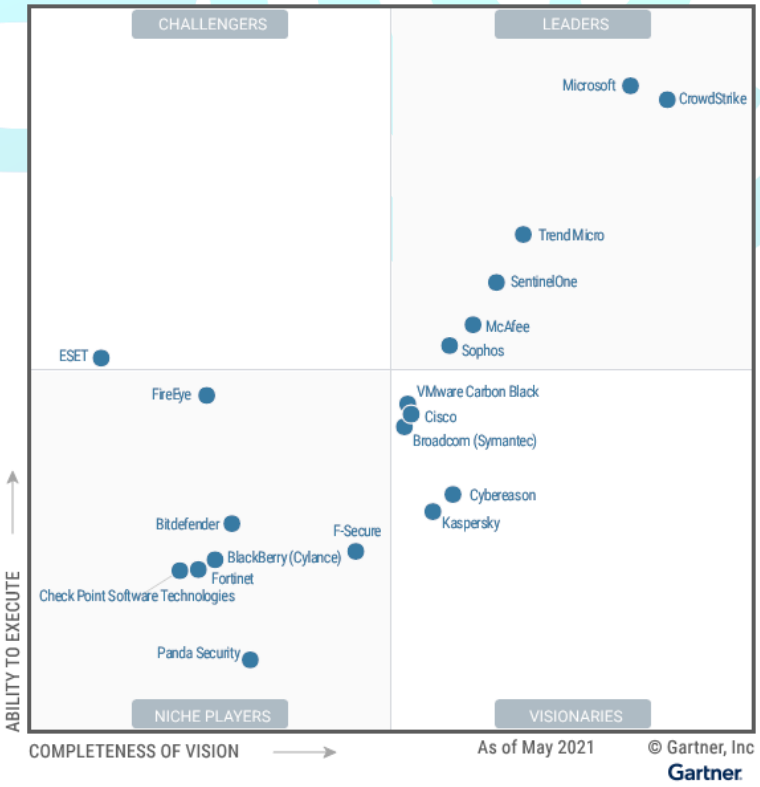
Once cybercriminals get past perimeter firewall defenses, they are free to roam a business production network searching for company resources to steal, encrypt, corrupt or hold hostage to disrupt business operations as leverage to achieve their financial or other self-serving objective.

This makes it imperative to **stop trusting everyone** and everything in your business network, especially now that remote workers are accessing company networks from home systems that may not be as secure as needed for the company's purposes.

Zero Trust assumes no one can be trusted and that any user or device seeking network access is already compromised and uses deny-by-default settings requiring validated credentials to access both the network and any resources needed to perform their required functions. They only receive permission to use the resources so required and have no access to other resources on the network. This requires complete network visibility and granular access controls.

- **Get proactive about endpoint protection.**

Here's how prominent research firm Gartner recently rated the major endpoint detection and response (EDR) providers. Managed Detection and Response (MDR) providers (see list here) also staff EDR systems for clients, a major benefit for those without qualified in-house IT staff.



Click Here to Find Funding for Your Cybersecurity Needs – Up to $33K Per Employee

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 4

How to Protect Your Smartphone from Hacking

Whether it is listening to a podcast on our way to work, doing quick calculations as our mental math skills have almost completely deteriorated, or putting everything from movies to doctors' appointments in our calendar, there is hardly ever a moment when we do not have our smartphone by our side.

So, if we were to be hacked, we would be in deep trouble, risking information about our credit and debit cards, location, social security number, and more. And so would the employers of those using their smartphones to access company information systems, since they are exposed to even more cyber threats by virtue of these back doors into their IT systems.

There are several ways to prevent hackers from gaining access to smartphones, and none of them require much time or effort. In just a few minutes, you can go from zero to hero regarding smartphone security. Let's get started!

a. Do Not Jailbreak.

No, this is not a game of Monopoly. Jailbreaking your smartphone means that you have complete control over your smartphone, avoiding the manufacturer's restrictions. So, on an iPhone, for example, that means you will be able to use apps from places other than Apple's official app store, plus make any tweaks to your phone's iOS.

However, we do not recommend jailbreaking because with freedom comes lack of security. First, you should not be downloading apps that are not from the app store, as they have not been screened for malware.

In fact, when you jailbreak your phone, you are basically taking down all the security measures that the manufacturer has built into their smartphones - think of it like bulldozing the fence around your house.

b. Make Smartphone Lock Sooner.

You might have noticed that when you don't have your smartphone on hand it will lock, forcing you to enter your passcode or biometrics like your fingerprint or face.

While it might be annoying to have to sign in every time, ultimately it is protecting your device so we recommend setting your auto-lock to 30 seconds, meaning it will lock with no activity for 30 seconds. And if you do not have the lock turned on at all, needless to say, you should probably change that.

c. Perform All Software Updates.

Companies like Google and Apple have people working around the clock to improve the smartphone's security, so if there is ever an iOS or Android update, do it.

Although these updates can be annoying, they are incredibly necessary for keeping up with the latest and greatest in security software. Doing them at night will mean you are never without your smartphone in your waking hours!

d. Set Up Two-Factor Authentication.

If you have been paying attention, then you know that it is a smart idea to turn on auto-lock, so you'll have to enter a passcode to access your smartphone. But if you want to take that a step further, set up two-factor authentication.

That way, if someone guesses your passcode, they still will not be able to access your phone as your phone company will send you another code via text or phone call. Again, this will make opening your smartphone a bit more tedious, but it is a prudent idea if you are serious about avoiding hackers.

e. Create Long Passcode.

When choosing a passcode, people tend to use something obvious like their birthday, numbers in chronological order, or a portion of their phone number. This is not the safest practice.

Rather, the numbers should be truly random, and be sure to use a six-digital passcode, the longest possible. While it will be a bit harder to remember this number, it will also be harder for hackers to guess, which is ultimately a good thing for your phone's security and any business systems you access with your phone.

f. Turn On Erase Data.

Now what if your smartphone is lost or stolen and, for some reason, your hackers can access your account? Of course, this is a worst-case scenario, but thinking about what to do in these situations is what this report is all about.

The solution? Turn on Erase Data, otherwise known as setting your smartphone to self-destruct. The other option is having the phone automatically "self-destruct" after too many failed passcode attempts. Of course, this is more extreme, but will certainly increase your smartphone's security.

g. Avoid Phishing and Pop-Ups.

Phishing has gotten increasingly sophisticated, sending tech-savvy people ostensibly legitimate links and pop-up ads. While phishing is a topic addressed elsewhere in this report, there are some basics that are relevant to smartphone security.

Do not email any sensitive information unless you are sure of the recipient, and don't click on any links unless you are sure they are legitimate. Scroll down below for more on how to tell if a website is safe or not.

h. Turn Auto-Fill Off.

Auto-fill, which fills out forms automatically with your personal and financial information, is both incredibly convenient and incredibly dangerous if your phone ends up in the wrong hands.

While it might make your life a bit more tedious, it is a safe idea to turn off auto-fill on your smartphone.

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 5

A Guide to Types of Malware and How to Handle Them

Malware, short for "malicious software," is any unwanted software on your computer that is most often designed to inflict damage. Since the early days of computing, a wide range of malware types with varying functions have emerged.

At its core, malware exploits existing network, device, or user vulnerabilities, posing as little risk as annoying advertisements to much more damaging demands for millions in ransom payments.

Here are some common and not so common malware threats and how to defend against them.

a. Adware

Adware, also known as "malvertising", is a type of malware that downloads or displays advertisements to the user interface. Rather than stealing data, adware is more of an irritant forcing users to see unwanted ads.

Most users are familiar with adware as unclosable browser pop-ups. Users may unknowingly infect themselves with adware installed by default when downloading and installing other applications.

How To Defend Against Adware

Install an antivirus solution that includes anti-adware capabilities. Disable pop-ups on your browsers and pay attention to the installation process when installing new software, making sure to un-select any boxes that will install additional software by default.

b. Backdoors

A backdoor is a trojan that offers an attacker remote access into the victim's device. Most device or software manufacturers place backdoors in their products intentionally and for a good reason. If needed, company personnel or law enforcement can use the backdoor to access the system when needed for updates, bug fixes, etc.

However, in a bad actor's hands, a backdoor can do anything the user does. Backdoors can also be installed by other types of malware like viruses or rootkits.

How To Defend Against a Backdoor

Backdoors are among the most challenging types of threats to protect against. Experts say the best defense is a multi-pronged network security strategy that includes a firewall, anti-malware software, network monitoring, intrusion detection and prevention (IDPS), and data protection.

c. Bots and Botnets

Bots are software performing automated tasks, making attacks known as “botnets” extremely harmful for victims. In cybersecurity, a bot typically refers to an infected device containing malicious software.

Without the user’s knowledge or permission, a bot can corrupt the device. Botnet attacks are targeted efforts by an army of bots, directed by their bot herder.

How To Defend Against Botnets

Organizations can help prevent their computers from becoming part of a botnet by installing anti-malware software, using firewalls, keeping software up-to-date, and requiring users to use strong passwords.

Network monitoring software can also help determine when a system has become part of a botnet. Always change the default passwords for any IoT devices you install before extended use.

d. Browser Hijacker

A browser hijacker, also called “hijackware,” noticeably changes the behavior of your web browser. This change could be sending you to a new search page, slow loading, changing your homepage, installing unwanted toolbars, directing you to sites you did not intend to visit, and displaying unwanted ads.

Attackers can make money off advertising fees, steal information from users, spy, or direct users to websites or apps that download more malware.

How To Defend Against a Browser Hijacker

Be careful when installing new software on your system. Many browsers’ hijackers piggyback on wanted software, much like adware does. Ensure you install and run anti-malware software on your system and maintain high-security settings for browser activity.

Because hijackware is related to your browser, therein lies the solution to exterminating a browser hijacker. If your antivirus software fails to notice a new strain, you can reinstall the browser. If that fails to work, clearing the contents of the device might be required.

e. Bugs

Bugs are a generic term for flaws in segments of code. All software has bugs, and most go unnoticed or are mildly impactful to users. Sometimes, however, a bug represents a severe security vulnerability and using software with this type of bug can expose your system to attacks.

How To Defend Against Bugs

The best way to minimize potentially nasty bugs is consistently updating for your software. With vulnerabilities at the top of software vendors' minds, they are quick to release patches to prevent user systems damage.

For organizations writing or configuring their code, it is imperative to follow best practices for secure code and potentially seek third-party review.

f. Crimeware

Some vendors use "crimeware" to refer to malware that is criminally executed and often financially benefits the attacker. Much like malware, it is an inclusive category that encompasses a wide variety of malicious software.

Unlike ransomware, it might be a criminal operation that does not involve the collection of a ransom. As a term, crimeware encompasses much of the malware types listed in this article.

How To Defend Against Crimeware

Best network security practices are essential, including using anti-malware, firewalls, intrusion prevention and detection (IPDS), network and log monitoring, data protection, security information and event management (SIEM) and threat intelligence.

Cybersecurity vendors suggest the best way to defend against crimeware is using a combination of antivirus, anti-spyware, firewalls and threat detection technology.

g. Keyloggers

A keylogger is a software program that records all of the keys a user touches. This exposed data includes everything from emails and text documents to passwords entered for authentication purposes. By obtaining sensitive authentication access, attackers can break into the vendor network or user account.

How To Defend Against a Keylogger

Good password hygiene is one of the best ways to prevent access to keyloggers. Using strong passwords that you update regularly can go a long way towards keeping you safe. You should also use a network firewall and an anti-malware solution.

h. Malicious Mobile Apps

In the sea of apps available today, not all of them are desirable, and the problem is even more acute with third-party app stores. While app store vendors try to prevent malicious apps from becoming available, some inevitably slip through. These apps can steal user information, attempt to extort money from users, gain access to corporate networks, force users to view unwanted ads, or engage in other undesirable activity types.

Preventing Damage from a Malicious Mobile App

User education is one of the most powerful tools for preventing malicious mobile apps. By avoiding third-party app stores and investigating app data before downloading, users can significantly mitigate this risk. Deploying mobile anti-malware and a company-wide mobile security plan is essential for large organizations.

i. Phishing and Social Engineering

Phishing and social engineering are types of email attacks that trick users into divulging passwords, downloading attachments, or visit websites that install malware on their systems.

More targeted efforts at specific users or organizations are known as spear phishing. Because the goal is tricking users, attackers research victims to maximize trick potential.

Preventing a Phishing attack

Because phishing relies on social engineering — tricking users into doing something — employee training is one of the best defenses against these attacks. Users should deploy anti-spam and anti-malware solutions, and staff should know not to divulge personal information or passwords in email messages.

Training about downloading attachments or clicking website links in messages, even if they appear to come from a known source, is imperative given that phishing attackers often pretend to be a company or person known to the victim. Email is also usually how ransomware works.

j. RAM Scraper

RAM scraper malware, also known as Point-of-Sale (POS) malware, harvests data temporarily stored in a system's memory, also known as random access memory (RAM). This type of malware targets point-of-sale (POS) systems like cash registers or vendor portals where an attacker can access unencrypted credit card numbers. While this sensitive payment data is only available for milliseconds before passing the encrypted numbers to back-end systems, attackers can still access millions of records.

Preventing a RAM Scraper

Organizations can help prevent RAM scraper attacks by using hardened POS systems and separating payment-related systems from non-payment systems. Usual precautions such as anti-malware software, firewalls, data encryption, and complying with any relevant standards or regulations for protecting customer data are a must.

k. Ransomware

Ransomware has quickly become one of the most prevalent types of malware. The most common malware variants encrypt a system or specific files, pausing any work from being done until the victim pays a ransom to the attacker. Other forms of ransomware threaten to publicize sensitive information within the encrypted data.

Preventing Ransomware

Organizations can mitigate ransomware attacks with up-to-date and secure backups. If their files become locked, they can wipe the system and reboot from an offline backup. Organizations should train users about the threat, patch their software as necessary and install all the usual security solutions. Some instances of ransomware appear so dire that many organizations and individuals resort to paying the ransom even though their attackers may not restore their data access or even be able to decrypt it for them.

l. Rootkit

Rootkits are one of the most insidious malware types because they allow attackers to have administrator-level access to systems without users' knowledge. Once an attacker has root access to a network, they can do almost anything with the system, including recording activity, changing system settings, accessing data, and attacking other systems.

Preventing a Rootkit

You can prevent most rootkit infections by installing appropriate security software (anti-malware, firewall, log monitoring) and keeping operating systems and other software up to date with patches. Be careful when installing any software on your system and when clicking email attachments or links. If a rootkit infects your system, it can be nearly impossible to detect and remove. In many cases, you may have to wipe your hard drive and start over from scratch to get rid of it.

m. Spyware

Spyware is software that gathers information about someone without their knowledge or consent (e.g., website tracking cookies that monitor users' browsing history is considered spyware). Other spyware types might attempt to steal personal or corporate information.

Government agencies and law enforcement often use spyware to investigate domestic suspects or international threat actors. It is challenging for the user to detect spyware symptoms ranging from performance issues to unusual modem activity.

Preventing Spyware

Install anti-spyware software on your computer. Luckily, anti-spyware capabilities are included in most antivirus or anti-malware packages. Using a firewall and caution when downloading software is a must. And, finally, scanning for potential threats at least once a week can be a lifesaver.

n. Trojans

In computer security, a trojan is any malware that pretends to be something else but serves a malicious purpose. For example, a trojan might appear to be a free game, but once installed, it might destroy your hard drive, steal data, install a backdoor or take other harmful actions.

Preventing a Trojan

Because trojans use social engineering for targeted attacks, educating users is imperative. Caution when installing new software or clicking email links and attachments is the name of the game. Organizations can defend against most trojans with security software such as anti-malware software and sufficient firewalls.

o. Viruses

While some refer to malware and viruses interchangeably, a virus is a specific type of malware that requires human activation - a click on an attachment, image, link, or even a file accessed every day. Often hidden, a click by staff could unknowingly boot up a virus.

Viruses infect a device and then attempt to spread to other devices and systems. As far as damages go, a virus can perform several undesirable commands.

These include:

- Incorporating systems into a botnet
- Sending spam to contacts
- Stealing sensitive information
- Locking the system
- Missing files and programs

Preventing a Virus

Any internet-enabled system in your network should have antivirus software installed and up-to-date. Deploying a firewall is essential but use care when clicking on email attachments or URL links. Inspecting website security by its SSL is imperative to avoid visiting unknown or untrusted websites.

Major antivirus software vendors include CrowdStrike, Avast, AVG, Bitdefender, ESET, Norton, Panda and Sophos. Microsoft offers free Windows protection in the form of Microsoft Defender.

p. Worms

A worm is like a virus because it spreads itself, but a worm does not need an attacker's permission for activation. Instead, it is a standalone piece of malware that extends within a system or network. Like viruses, it can cause just as much damage to the device.

How To Defend Against Worms

As with viruses, the best way to prevent worm infections is with antivirus or anti-malware software. And as always, users should only click on email links or attachments when confident of the contents.

Prepare For All Malware Types

If you have made it this far, you know the forest of malware is dark and deep. Today's league of malicious actors isn't relying on the traditional forms of malware. They're consistently seeking more robust strains that can outdo your network security and current anti-malware or antivirus solutions.

Being aware of the dangers that lie in different types of malicious software comes first. As a business owner or manager, it is your responsibility to stay mindful of malware trends, actively respond to pertinent vulnerabilities and take proactive measures to prevent successful cyber-attacks.

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 6

How to Avoid Visiting Unsafe Websites

Given the number of times most of us use the Internet in a day, we probably spend comparatively truly little time thinking about which websites are safe to use. Of course, going to a bad website can have major consequences like phishing, viruses, malware, identity theft— you name it.

But how are you supposed to know when a website is unsafe, and what are some things you can do to make sure you are only visiting legitimate websites?

Here are a few quick signs that a website is okay to use:

- Padlock symbol next to URL
- HTTPS in URL rather than HTTP
- Privacy policy on website
- Website accepts all major payment methods.

When you are surfing the web, it is important to look for red flags like:

- Browser tells you the website is unsafe.
- Many pop-ups or redirects to other shady looking websites.
- Website only accepts bank transfers or wire payments.
- No return policy or privacy policy on the website.

Let's dive in a little deeper.

a. In-Browser Tools for Website Safety

Chances are that your browser already does a lot for you in terms of seeing which websites are safe. The Chrome browser, for example:

- Blocks pop-ups
- Sends "do not track" requests to websites to protect our data.
- Disables unsafe flash content.
- Stops malicious downloads.
- Controls which sites can access our speaker, microphone, and camera.

Simply go into your browser's settings and check in the "Privacy and Security" section to see how your browser filters out the bad. Of course, these built-in browser safety tools do not catch everything, which is why it is important to perform other tests.

b. Other Website Safety Tests

If you are not feeling confident that a website is safe, the easiest thing to do is enter it into a website checker like the Google Transparency Report, the Norton Safe Web Checker URLVoid or comparable tool. It will tell you whether the website is safe or not in under two seconds!

c. Use Trusted Retailers

This one may seem obvious, but especially if you are doing any online shopping, try to use retailers who you have heard of - Amazon being the most obvious choice. Remember, you are giving this site your credit or debit card information along with your name, email, and address, which could be dangerous if it got into the wrong hands.

d. Double Check URLs

Sometimes, scammers will misspell names of trusted URLs or replace one of the letters with a number, like writing google.com (using zeros instead of the letters “o”) instead of google.com. In a rush, this is something you can easily miss, and with fake websites imitating real websites as well as they do, it’s pretty easy to give your personal information to the bad guys.

Luckily, if you use Firefox or Chrome, you can simply hover your mouse over the “anchor text” (AKA the text that is linked), to see the URL before you click on it; it’ll show up in the bottom left-hand corner of your browser.

e. Note Payment Methods

Check that the website accepts all major credit and debit cards. Any normal website will have normal payment methods from the major credit/debit card companies, like Mastercard, Visa, American Express. If a website only accepts bank transfers or wire payments, steer clear.

f. Check Review Sites

The Internet is the perfect place for people to air out their problems to as many people as will listen. Chances are, if there is a subject, people have reviewed it on the web, from restaurants to e-commerce sites. Take advantage of people’s insatiable need to publicly rate everything and check review sites like TrustPilot, especially if it is an e-commerce site. You do not even necessarily have to use a review site. Simply ask Google if the website/company is a scam and see what people have said. If multiple people say it is a scam, they are most likely correct.

g. Check for HTTPS

Now, this is not 100% foolproof, but most reputable websites will have URLs that begin with HTTPS rather than HTTP; and yes, if you're wondering, the S does stand for secure. Basically, that tiny little letter is the difference between a secure website that encrypts your data and a scam website that steals it (with exceptions, of course).

If the website is secure, you will see a padlock to the left of the URL, but note that some unsafe websites have HTTPS, so it is not guaranteed to be safe. However, one hard and fast rule that you can follow is never enter your password or financial information on any website missing the padlock.

h. Look for a Privacy Policy

The truth is, most reputable websites have privacy policies, as many countries require them by law, so be sure to look for one on a website. Now, we are not saying you will be able to understand these policies, as they are often written in what those in the industry call "legalese".

But to get a good idea of how the website will use your data, press Control F and search for things like "third-party,", "data," "store," and "retain". If a website lacks a privacy policy at all, it's safest not to trust it.

i. Do Not Blindly Trust "Trust" Badges

Do you know how easy it is to get one of these so-called "trust badges" on your website? It is so easy that you can literally type in "trust badges" to Google images and drag them onto your site.

Although these seals may look legitimate, literally anyone could add them to their website, from huge companies to the shadiest "foreign prince" on the web. We are not saying these trust badges automatically make a site untrustworthy; however, you should not mistake them for security.

j. Look for These Red Flags

There are several red flags that not only make a website a poor user experience, but also might be a clue that something is amiss. Watch out for:

- Flash warnings
- Pop-ups
- Too many exclamation points!!!!!
- Redirects to other sites that look unsafe.
- Search engine warnings from your browser or search engine

- Bad spelling and grammar
- Illogical text
- Weird pictures
- No space to leave product reviews.
- No return policy or privacy policy on site
- Prices that are too good to be true.

As much as we hate to judge a book by its cover, these are all signs of a website that's not safe.

k. Look Up Domain Owner

Most reputable websites, particularly for businesses, will have a domain owner that's easy to lookup on ICANN's Domain Name Registration Data Lookup. This website will also tell you the date this registry expires, the organization and mailing address of the registrant, and the data the registry was created.

l. Call Company

We know it sounds old-fashioned, but even the most advanced robots have trouble mimicking humans exactly. Therefore, if you are not sure if a website is from a real company, an easy way to find out is simply by calling them over the phone.

Typically, most websites will provide a phone number either on their Contact or About Us pages. If you cannot find it, you can also try looking it up on the exact same who is lookup above or try contacting them through customer support.

m. Additional Web Security Tools

Finally, a straightforward way to avoid going to harmful websites is to use web security tools that protect you from viruses. Here are some top examples:

- AVG AntiVirus
- Avast Premium Security
- Norton 360 Standard
- CrowdStrike Falcon Prevent

With these software programs downloaded, you will not have to worry about giving your personal data to unsafe sites. It will do the work for you, so you don't have to worry about it.

n. VPNs

VPNs are Virtual Private Networks that encrypt your web traffic in a tunnel, completely hiding your web activity and replacing your IP address. They are especially useful if you are on a public network like a coffee shop, or if you simply want to access another country's server so you can enjoy Netflix Italy.

VPNs make it much less likely that your device will be hacked and you can easily download them onto your phone, tablet, computer, or even your router.

o. Identity Monitoring Services

Having your identity stolen can be one of the most emotionally and financially draining things you can go through, which is why it is important to employ an identity monitoring service. While none of them are guaranteed to completely prevent identity theft, they can monitor key areas that could indicate that your credentials have been stolen, such as your credit reports, bank, credit card and investment accounts, as well as the dark web and other criminal activity areas.

For example, if your name shows up on a sex offender registry, you will want to know about it. Same goes for if a new tax return is filed in your name. Plus, if your identity is stolen, most identity monitoring services will reimburse you for your losses for up to a million dollars.

p. Password Managers

Password managers make it easy to access your accounts by remembering your passwords for you - in a secure fashion of course. They are also great for storing important or sensitive information, and even automatically filling out web forms for you.

One of the most annoying things about technology is having to remember so many different passwords for different accounts. Plus, each account has its own rules, like you must have special characters, you cannot have numbers, no repeated letters and more, making it even harder to remember everything. And the process of resetting your password is less than fun, especially because you are probably just going to forget it again!

To conclude, being online does not have to be scary. There are many tools that can protect you online, like VPNs, password managers, identity monitoring services, and simply adjusting the settings on your devices. Knowing how to surf online safely is the first step to protecting your personal credentials and by following the above steps, you should be safe and secure.

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 7

Understanding Ransomware & Phishing and How to Prevent Them

Ransomware attacks via email are on the rise again, with several new and familiar forms of ransomware recently being distributed with the aid of malicious payloads in phishing messages.

Email used to be the most prolific way to infect victims with ransomware, but in recent years, attackers have successfully pivoted to using remote ports, insecure public-facing servers, and other vulnerabilities in enterprise networks to encrypt entire networks – often demanding hundreds of thousands of dollars and more in payments to release the data.

a. Ransomware Definition

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars for individuals to hundreds of thousands or millions for corporate victims, generally payable to cybercriminals in Bitcoin or other untraceable cryptocurrency.

b. How Ransomware Works

There are several vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust.

Once they are downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

In some forms of malware, the attacker may claim to be a law enforcement agency shutting down the victim's computer due to the presence of pornography or pirated software on it, and demand the payment of a "fine," perhaps to make victims less likely to report the attack to authorities.

But most attacks do not bother with this pretense. There is also a variation, called leakware or doxware, in which the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid.

But because finding and extracting such information is a very tricky proposition for attackers, encryption ransomware is by far the most common type of ransomware.

c. Who is a Target for Ransomware?

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it is a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet — and these organizations may be uniquely sensitive to leak ware attacks.

d. How to Prevent Ransomware Attacks

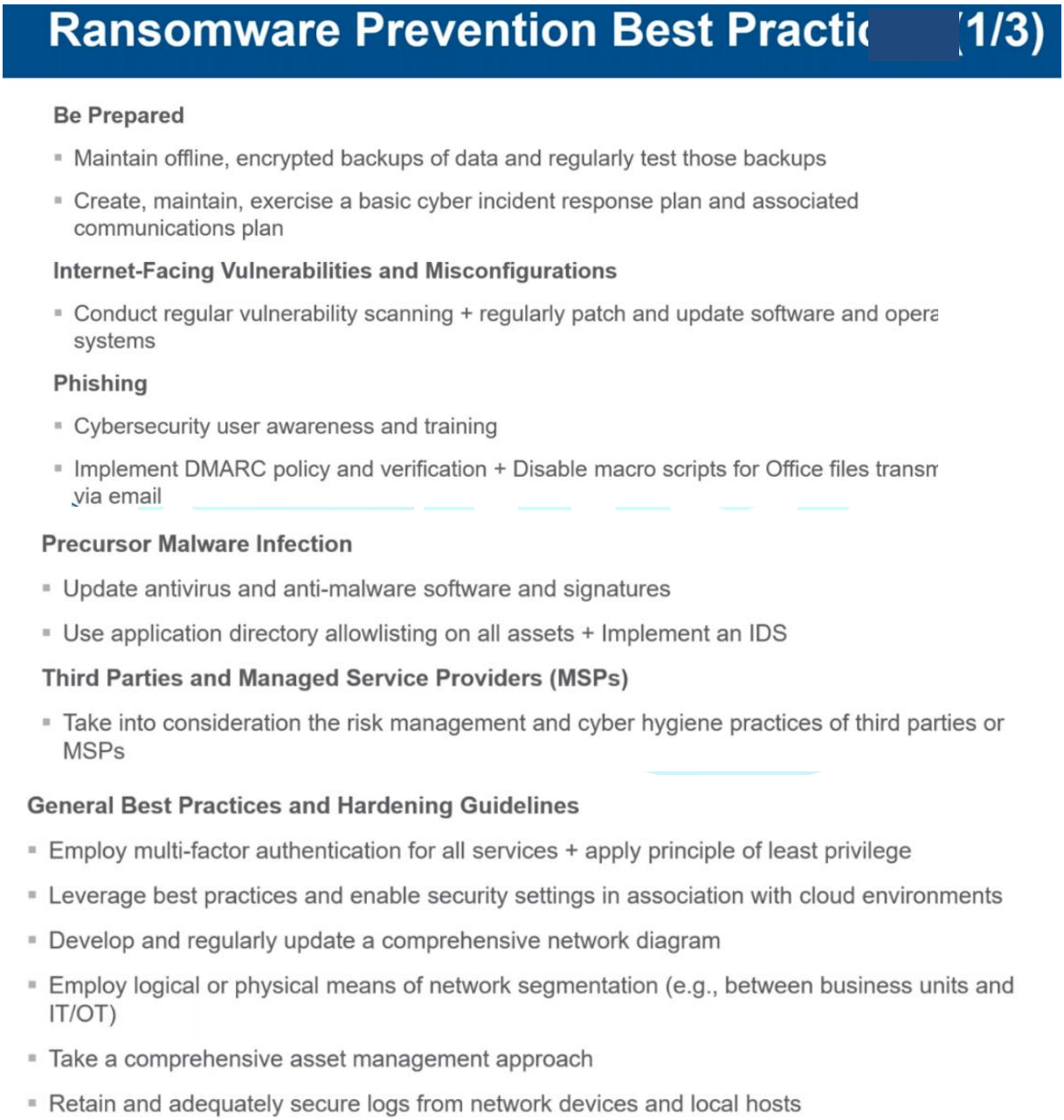
To protect yourself and your system(s) from ransomware, follow these recommended steps:

- Avoid opening unverified emails or clicking links embedded in them.
- Back up important files using the 3-2-1 rule: Create three backup copies on two different media with one backup in a separate location.
- Regularly update software, programs and applications to protect them from the latest vulnerabilities.
- Create a culture of security and equip personnel with adequate knowledge on ransomware and other threats that utilize phishing and unsecured accounts in their campaigns.
- Enforce the principle of least privilege to prevent users from running certain programs that can be used by ransomware variants.
- Limit access to shared or network drives and turn off file sharing. This minimizes the risk of a ransomware infection spreading to other devices.
- Keep your operating system patched and up to date to ensure you have fewer vulnerabilities to exploit.
- Do not install software or give it administrative privileges unless you know exactly what it is and what it does.
- Install antivirus software, which detects malicious programs like ransomware as they arrive, and whitelisting software, which prevents unauthorized applications from executing in the first place.

Organizations can also mitigate the effects of public shaming associated with ransomware double extortion schemes by taking the following steps when an attack has occurred:

- Notify law enforcement about the attack and the extent of the data breach.
- Follow data regulation protocols such as the General Data Protection Regulation (GDPR) and make the necessary disclosures and notifications.
- Prevent similar attacks from succeeding by addressing security issues exploited by the attack.

Before moving on to phishing, here are CISA's recommendations for preventing ransomware:



e. Phishing Definition

Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing the message is something they want or need - a request from their bank or note from someone in their company - and to click a link or download an attachment.

What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with. It is one of the oldest types of cyberattacks, dating back to the 1990s, and it's still one of the most widespread and pernicious, with phishing messages and techniques becoming increasingly sophisticated.

It uses social engineering techniques and computer programming to lure email recipients and Internet users into believing that a fraudulent website is legitimate. When the phishing victim clicks the phishing link, they find that their personal identity vital information, and even money, has been stolen.

The average cost of a phishing scam these days is $1.6 million, making it a top security concern for businesses today.

Some statistics:

- $70.2 billion is the estimated cost to brands, and
- $28.1 billion for corporations.

The occurrence:

- 3 billion each month
- 36 billion per year

The success rate:

- 1 in 3 companies is affected.
- 30% of phishing emails get opened.
- 100 million phishing messages get through every day.

Phishing is now the #1 vehicle for ransomware and malware. It is much more sophisticated and targeted than previously and is popular among cybercriminals because it usually succeeds.

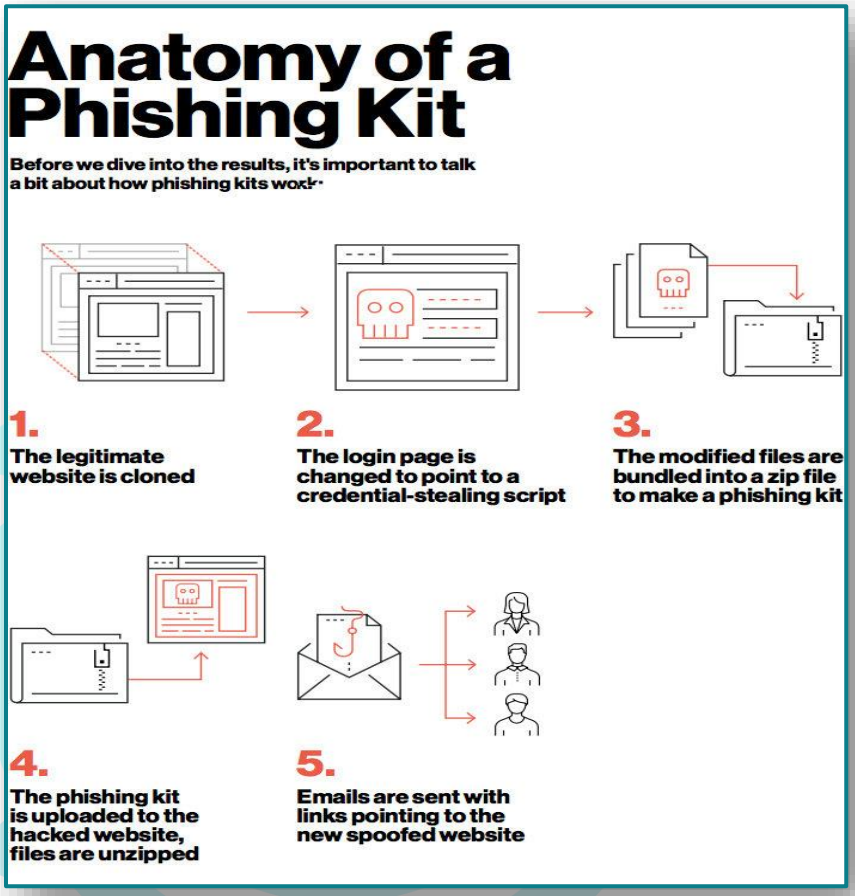
For every 10 messages sent there's a better than:

- 90% chance of being opened.
- 8% chance of users clicking on an attachment.
- 8% chance users will fill out a web form.
- 18% chance that users will click a malicious link in an email.

Even high-level executives get spoofed and share usernames and passwords.

f. What is a Phishing Kit?

The availability of phishing kits makes it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns. A phishing kit bundles phishing website resources and tools that need only be installed on a server.



Once installed, all the attacker needs to do is send out emails to potential victims. Phishing kits as well as mailing lists are available on the dark web. A couple of sites, Phishtank and OpenPhish, keep crowd-sourced lists of known phishing kits.

Some phishing kits allow attackers to spoof trusted brands, increasing the chances of someone clicking on a fraudulent link.

Analyzing phishing kits allows security teams to track who is using them. One of the most useful things we can learn from analyzing phishing kits is where credentials are being sent. By tracking email addresses found in phishing kits, we can correlate actors to specific campaigns and even specific kits.

g. Types of Phishing

If there is a common denominator among phishing attacks, it is the disguise. The attackers spoof their email address, so it looks like it's coming from someone else, set up fake websites that look like ones the victim trusts, and use foreign character sets to disguise URLs.

That said, there are a variety of techniques that fall under the umbrella of phishing. There are a couple of different ways to break attacks down into categories. One is by the purpose of the phishing attempt. Generally, a phishing campaign tries to get the victim to do one of two things:

1) Hand over sensitive information

These messages aim to trick the user into revealing important data — often a username and password that the attacker can use to breach a system or account. The classic version of this scam involves sending out an email tailored to look like a message from a major bank; by spamming out the message to millions of people, the attackers ensure that at least some of the recipients will be customers of that bank.

The victim clicks on a link in the message and is taken to a malicious site designed to resemble the bank's webpage, and then hopefully enters their username and password. The attacker can now access the victim's account.

2) Download malware

Like a lot of spam, these types of phishing emails aim to get the victim to infect their own computer with malware. Often the messages are "soft targeted" — they might be sent to an HR staffer with an attachment that purports to be a job seeker's resume, for instance. These attachments are often .zip files or Microsoft Office documents with malicious embedded code.

3) Spear phishing

When attackers try to craft a message to appeal to a specific individual, that is called spear phishing (think of a fisherman aiming for one specific fish, rather than just casting a baited hook in the water to see who bites.) Phishers identify their targets (sometimes using information on sites like LinkedIn) and use spoofed addresses to send emails that could plausibly look like they are coming from co-workers.

For instance, the spear phisher might target someone in the finance department and pretend to be the victim's manager requesting a large bank transfer on short notice.

4) Whaling

Whale phishing, or whaling, is a form of spear phishing aimed at the excessively big fish — CEOs or other high-value targets. Many of these scams target company board members, who are considered particularly vulnerable: they have a great deal of authority within a company, but since they are not full-time employees, they often use personal email addresses for business-related correspondence, which does not have the protections offered by corporate email.

Other types of phishing include clone phishing, vishing and snowshoeing.

h. How to Prevent Phishing Attacks

Here are 10 simple steps to identifying and preventing phishing scams.

1) Know what a phishing scam looks like

There are many sites online to stay informed about new phishing attacks and their key identifiers. The earlier you find out about these attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

2) Do not click on that link

It is generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one.

Some phishing attacks are sophisticated and destination URLs can look like a carbon copy of genuine sites, set up to record keystrokes or steal login/credit card information. If possible, go straight to the site via your search engine rather than clicking on the link, then you should do so.

3) Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there is no reason not to have this installed on every device in your organization.

4) Do not give your information to an unsecured site

If the URL of the website doesn't start with "https", or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.

5) Rotate passwords regularly

If you have online accounts, you should get into the habit of regularly rotating your passwords to prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

6) Do not ignore updates

Receiving numerous update messages can be frustrating and it can be tempting to put them off or ignore them altogether. Do not do this.

Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security.

If you do not update your browser and software, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

7) Install firewalls

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

8) Do not be tempted by those pop-ups

Pop-ups are not just irritating they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups.

If one does manage to evade the ad-blocker, though, do not be tempted to click on it. Occasionally pop-ups will try to deceive you with where the "Close" button is, so always try and look for an "x" in one of the corners.

9) Do not give out important information unless you must

As a rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your credit card information.

Make sure, if you must provide your information, that you first verify the website is genuine, that the company is real and that the site itself is secure.

10) Have a data security platform to spot signs of an attack

If you are unfortunate enough to be the victim of a successful phishing attack, then it is important that you can detect and react in a timely manner. Having a data security platform in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files.

If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 8

Tips for Creating the Right Post-Pandemic Cybersecurity Budget

As organizations start planning their cybersecurity budgets, it is immediately obvious that this year will bring new and unexpected costs. The global move to work-from-home (WFH) over the past year has left many organizations struggling to protect newly remote staff from a wider and more dynamic threat landscape.

In this chapter, we look at several key items that should be in your cybersecurity budget.

a. Threat Assessment

Every cybersecurity budget should be based, ultimately, on the level and types of threats you face. The COVID-19 pandemic has led to a noticeable uptick in cybercrime, while simultaneously forcing employees to work from home, where they are more vulnerable. The bottom line is, therefore, that cybersecurity will cost a lot more in the coming years than it did in the past.

This headline notwithstanding, it is as important as ever to conduct a thorough threat analysis for your organization - following best practice guidelines for this - before deciding which of the following budget items applies to you and how much you should spend on them. This threat assessment will also help to justify your cybersecurity budget this year in the event that management questions why it is so much higher than in previous years.

b. Staff and Training Costs

Before the pandemic, plenty of companies were in the process of moving to remote work. One of the driving forces behind this shift was the perception that WFH staff cost less than traditional staffing models. It turns out that is not the case, at least when it comes to cybersecurity.

This is because staff members who work from home require significant extra training to keep their and company's digital assets safe. Given the widespread skills shortage still characterizing the cybersecurity world, this is likely to apply to all teams. Even worse, if staff are not trained adequately, you will have to pay to clean up after their mistakes, which will cost even more.

c. Incident Response

Second, you should consider your risk tolerance, make a reasonable estimate of how many incidents you are likely to have to respond to this year, and how much this will cost. In many organizations, these costs are overlooked because cybersecurity consultants still make the mistake of thinking that spending enough on prevention will allow them to cut incident response costs to zero. Do not make that mistake. It just does not work like that.

d. Resource Replacement and Upgrade

You should also consider replacing and upgrading your hardware and software resources in response to the shift to WFH. Older laptops with out-of-date security software might be (barely) secure enough to protect your employees and data if they stay behind your corporate firewall, but once they leave the office they are exposed to a much higher level of risk on the open internet.

For this reason, now might be the time to replace aging hardware with newer machines that incorporate biometrics, or to install hardware encryption on older machines. Equally, this year is a good time to take a second look at any free but insecure software you might be using.

e. Consultants

This might seem like a bad time to spend thousands of dollars on consultants, but red-hat testing is a great way of understanding the threats you face and understanding how to mitigate them. Research shows that internal battles still hold SOC back in many firms, and a successful pen test is a great way to get everybody focused on the same goal.

f. Insurance

You have probably noticed that your cybersecurity insurance premiums have risen in the last year, and there is a good reason for that. Insurance companies have looked at the statistics and decided that remote employees present a huge risk. They are, accordingly, charging more to insure them, and you should make sure that your cybersecurity budget reflects this.

If, on the other hand, you do not currently have cybersecurity insurance at all, you should seriously consider getting it. While an extra expense might seem like a heavy burden to bear now, the savings in the event of a successful attack far outweigh this repeating, predictable cost.

g. Security-as-a-Service

Finally, and particularly if the number of factors above seems like it will increase your budget to unmanageable levels this year, it might be time to consider outside help. While there have been third-party security solutions on the market for decades, some have been developed into full-spectrum Security-as-a-Service platforms.

Others, like CrowdStrike's Security Operations Center-as-a-Service (SOCaaS) go even further in providing a fully staffed comprehensive security operations center, overcoming the difficulty of finding and recruiting competent trained professionals for this sophisticated work.

These platforms promise to take care of your cybersecurity in its entirety, leaving you free to focus on other priorities to grow your business.

h. Expect the Unexpected

While it might not feel like it right now, the kind of root-and-branch assessment of cybersecurity budgets necessitated by the pandemic might, overall, be a positive development. Many firms have not looked at their budgets and the assumptions they are based on for many years. For them, this review has been long overdue – especially as cybersecurity intrusions have skyrocketed during that time and more employees working from home has created much greater and more porous attack surfaces for company systems and data that raise the corporate risk profile substantially.

The process of looking afresh at your budget to reassess this growing risk and budget accordingly to build the required mitigation measures into your budget is simply responsible business and risk management.

i. New Sources of Cash Flow

If your budget lacks the resources to adequately fund the cybersecurity initiatives your business requires to remain reliably operational, there are other ways to close the funding gap.

U.S. government tax incentives remain largely overlooked by most small and midsize businesses, many of which are eligible for hundreds of thousands of dollars and more in combined cash flow benefit – some of it immediate and none of which requires repayment.

These **employer incentives** include:

- Employee Retention Credits (ERC) of up to $33,000 per employee retained through 12/31/21.
- Work Opportunity Tax Credits (WOTC) of up to $9,600 per eligible new hire; and
- Research and Development (R&D) Credits for creating or improving new products or processes.

There are more – you can get an initial estimate of how much your company may be eligible to receive here.

Click Here to Find Funding for Your Cybersecurity Needs – Up to $33K Per Employee

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 9

How Should Companies Adapt Their Post-Pandemic Cybersecurity Strategy?

Many companies are struggling to adapt their security strategy to accommodate the new normal. With remote working now an ongoing reality, there has been a rush to adopt and integrate a slew of new tools and cloud platforms to facilitate collaboration and maintain productivity.

However, in the race to connect everyone, security implications are often overlooked. This, coupled with the fact that relying solely on a corporate firewall is no longer a sound security strategy, puts many organizations at risk.

What should companies do to adjust their security strategy? Here are five practical steps to take to prevent cybercriminals from taking advantage of an extended virtual business environment.

a. Adopt a Zero Trust Approach

Organizations need to adopt a Zero Trust mindset, strategy and culture now that there is no longer a well-defined security perimeter. According to this *Forbes* article, "Organizations need to reset their security to a deny-by-default status. Any user or device that wants access needs to provide validated credentials to the network before being granted that access. And then, they are only given permission to use those resources that are specifically required to do their job."

All systems must require authenticated access from an authorized individual or device, whether or not they reside on the company's internal or external network. Businesses should also require remote employees to use a virtual private network (VPN) to access corporate resources when not physically in the office. This will help mitigate security concerns, although the *Forbes* article lists VPN shortcomings that reinforce the need for Zero Trust measures.

b. Review Security Before Adding Tools

There has been a surge in the adoption of collaboration tools and cloud services to support engagement in our digitally dependent world, especially as remote work from home has become more prevalent with the COVID pandemic. Most organizations have prioritized convenience over security concerns. Rather than rushing to adopt new collaboration tools, IT teams need to audit every such solution for potential security vulnerabilities and know how to securely configure them before they are activated.

In addition, teams must adjust their approach from security enforcer to taking on the persona of a risk advisor - helping the business and its employees understand the security vulnerabilities while supporting a more agile response to the new working environment.

c. Make Multi-Factor Authentication Mandatory

Passwords remain a weak link and are the source of many cybersecurity vulnerabilities. Sensitive systems and data require more than a simple password for security. Organizations need to add additional layers without introducing too much friction to the user experience rather than hoping that one will suffice.

d. Tap into Intelligent Technologies

With the shortage of cybersecurity resources along with escalating threats, harnessing the power of intelligent technologies has never been more critical.

The ability of these solutions to process vast volumes of data to identify and predict threats is an invaluable resource for organizations that shouldn't be overlooked. Machine learning and bot detection are critical tools for post-pandemic security teams.

e. Practical Security Training for Remote Workers

Security training is critical so that employees understand the new risk landscape. Training should aim to help protect both professional and personal data as most home networks are overloaded with a range of different devices. Employees will be more receptive if you present a holistic view of the threats. There need to be regular tips and tricks that educate employees on the latest cyber scams and phishing attacks to prevent employees from falling for lures.

Setting up a chatbot to address frequently asked questions from remote workers will provide employees with the information they need when they need it without adding any unnecessary burden on the IT team.

The working environment has changed forever and organizations need to adopt an agile approach to deal with the new threat landscape. Staying rooted to what worked in the past has the potential to be a recipe for disaster when it comes to cybersecurity.

Cybersecurity Training Guide for U.S. Businesses

CHAPTER 10

Case Studies

Ransomware, phishing, and ATM skimming are just a few common and very damaging cybersecurity threats that small and midsize businesses need to watch for. The following case studies were created by the National Cyber Security Alliance, with a grant from NIST, and should prove useful in stimulating ongoing learning for all business owners and their employees.

a. Case 1: A Business Trip to South America Goes South

SCENARIO:

A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the U.S., the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $13,000, all originating from South America. There was an additional $1,000 overdraft fee.

ATTACK:

The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.

What is Skimming? Skimming occurs when criminals install devices on ATMs, point-of-sale (POS) terminals, fuel pumps, etc. to capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts.

RESPONSE:

Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful.

The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the $1,000 overdraft fee from the firm owner's personal account.

The firm severed ties with that bank. The new bank offered comprehensive fraud protection guarantees.

The firm created two business accounts:

- one for receiving funds and making small transfers.
- one for small expense payments.

The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically, pay cash, or use a major credit card, as necessary.

IMPACT:

The entire cash reserve for the small business was wiped out, netting losses of almost $15,000.

LESSONS LEARNED:

- Use major credit cards when traveling - they have more consumer fraud protection than debit cards.
- Get notified - set up transaction alerts with your credit and debit card companies to monitor fraud.
- Check your bank account frequently.
- Create withdrawal alerts.
- Understand your bank's policies about covering losses from fraud.

b. Case 2: Construction Company Hammered by a Keylogger

SCENARIO:

A small family-owned construction company made extensive use of online banking and automated clearing house (ACH) transfers. Employees logged in with both a company and user-specific ID and password and answered two challenge questions for transactions over $1,000.

The owner was notified that an ACH transfer of $10,000 was initiated by an unknown source. They contacted the bank and identified that in just one-week cyber criminals had made six transfers from the company bank accounts, totaling $550,000. How? One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account.

ATTACK:

Cyber criminals were able to install malware onto the company's computers, using a keylogger to capture the banking credentials.

A keylogger is software that silently monitors computer keystrokes and sends the information to a cybercriminal. They can then access banking and other financial services online, using valid account numbers and passwords.

RESPONSE:

The bank was able to retrieve only $200,000 of the stolen money in the first weeks, leaving a loss of $350,000. The bank even drew over $220,000 on the business' line of credit to cover the fraudulent transfers. Not having a cybersecurity plan in place delayed the company response to the fraud.

The company also sought a cybersecurity forensics firm to:

- Help them complete a full cybersecurity review of their systems.
- Identify what the source of the incident was.
- Recommend upgrades to their security software.

IMPACT:

The company shut down their bank account and pursued legal action to recover its losses. The business recovered the remaining $350,000 with interest. No money for time and legal fees was recovered.

LESSONS LEARNED:

- Get notified - set up transaction alerts on all credit/debit cards and bank accounts.
- Restrict access to sensitive accounts to only those employees who need access and change passwords often.
- Companies should evaluate their risk and evaluate cyber liability insurance options.
- Choose banks that offer multiple layers of authentication to access accounts and transactions.
- Create, maintain, and practice a cyber incident response plan that is rapidly implementable.
- Cyber criminals deliver and install malicious software via email. Train employees on email security.

c. Case 3: Stolen Hospital Laptop Causes Heartburn

SCENARIO:

A health care system executive left a work-issued laptop with access to over 40,000 medical records in a locked car while running an errand. The car was broken into, and the laptop stolen.

ATTACK:

Physical theft of an unencrypted device. Encryption is the process of scrambling readable text so it can only be read by the person who has the decryption key. It creates an added layer of security for sensitive information.

RESPONSE:

The employee immediately reported the theft to the police and to the healthcare system's IT department who disabled the laptop's remote access and began monitoring activity. The laptop was equipped with security tools and password protection. Data stored on the hard drive was not encrypted – this included sensitive, personal patient data. The hospital had to follow state laws as they pertain to a data breach.

The U.S. Department of Health and Human Services was also notified. Personally Identifiable Information (PII) and Protected Health Information (PHI) data require rigorous reporting processes and standards.

After the theft and breach, the healthcare system began an extensive review of internal policies; they created a discipline procedure for employees who violate security standards. A thorough review of security measures with internal IT staff and ancillary IT vendors revealed vulnerabilities.

IMPACT:

The healthcare system spent over $200,000 in remediation, monitoring, and operational improvements. A data breach impacts a brand negatively and trust must be rebuilt.

LESSONS LEARNED:

- Companies must establish and train employees on secure handling of work-issued devices.
- Devices must be safely stored when not in the immediate presence of the employee.
- Companies must take steps to encrypt data wherever it is stored or transmitted. Employees should have a clear understanding of the importance of encryption and how to use it.
- Companies must understand and know their responsibilities under the data breach notification laws of the state(s) in which they operate.

- A regular review of company security practices is imperative in modern organizations to prevent incidents, discover vulnerabilities and to reduce impact of incidents.

d. Case 4: Hotel CEO Finds Unwelcome Guests in Email Account

SCENARIO:

The CEO of a boutique hotel realized their business had become the victim of wire fraud when the bookkeeper began to receive insufficient fund notifications for regularly recurring bills. A review of the accounting records exposed a serious problem. At some point a few weeks before, the CEO had clicked on a link in an email that he thought was from the IRS. It was not.

When he clicked the link and entered his credentials, the cyber criminals captured the CEO's login information, giving them full access to intimate business and personal details.

ATTACK:

Social engineering, phishing attack.

A phishing attack is a form of social engineering in which cyber criminals trick individuals by creating and sending fake emails appearing to be from an authentic source, such as a business colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with malware.

RESPONSE:

The hotel's cash reserves were depleted with fraudulent transfers of more than $1 million. The hotel also contacted a cybersecurity firm to help them mitigate the risk of a repeat attack.

IMPACT:

The business lost $1 million to an account in China. The funds were not recovered.

LESSONS LEARNED:

- Teach staff about the dangers of clicking on unsolicited email links and attachments and the need to stay alert for warning signs of fraudulent emails. Engage in regular email security training.
- Implement stringent wire transfer protocols and include a secondary form of validation.
- Have a cyber incident response plan ready to implement.

e. Case 5: Dark Web of Issues for Small Government Contractor

SCENARIO: The CEO of a government contracting firm was notified that an auction on the dark web was selling access to their firm's business data, which included access to their military client's database. The CEO rapidly established the data being "sold"' was obsolete and not tied to any government agency clients.

How did this happen? The firm identified that a senior employee had downloaded a malicious email attachment, thinking it was from a trusted source.

ATTACK:

A phishing attack where malware is in the attachment of the email.

A phishing attack is a form of social engineering in which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source such as a business or colleague.

The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with a virus or malware.

RESPONSE:

The company's IT management immediately shut off communications to the affected server and took the system offline to run cybersecurity scans of the network and identify any additional breaches. They hired a reputable cybersecurity forensics firm and impacted government agencies were notified. The U.S. Secret Service assisted in the forensics investigation.

IMPACT:

The operational and financial impact from the breach was extensive – costing more than $1 million. The company was offline for several days disrupting business. New security software licenses and a new server had to be set up.

LESSONS LEARNED:

- You are never too small to be a target. A cyber-attack can happen to anyone.
- Teach staff about the dangers of clicking on unsolicited email links and attachments and emphasize the need to stay alert for warning signs of fraudulent emails.
- Install and regularly update anti-virus, network firewall, and information encryption tools to scan for and counteract viruses and harmful programs.
- Conduct ongoing vulnerability testing and risk assessments on computer networks.

Cybersecurity Training Guide for U.S. Businesses

Conclusion

As we move into a post-pandemic business economy, one thing remains clear - cyber threats will not only remain a threat to business operations and profitability but will grow in scope. Cyberattacks have also grown in sophistication and complexity.

The days of simply relying on your computers' built-in antivirus software are over. Businesses need the best endpoint security software and a good deal more to remain protected.

Organizations will need to remain vigilant about remote work policies, data access, and upskilling, and they will need to rely on the security technologies that incorporate Artificial intelligence (AI) and cloud security. The challenges are there, but so are the opportunities.

With the strategies and information provided in this training guide, you know enough to protect your business from online threats and ensure the protection of your digital and financial assets.

To summarize the appropriate mindset for preventing cyber intrusions into your business or personal information, it helps to remember the old adage…

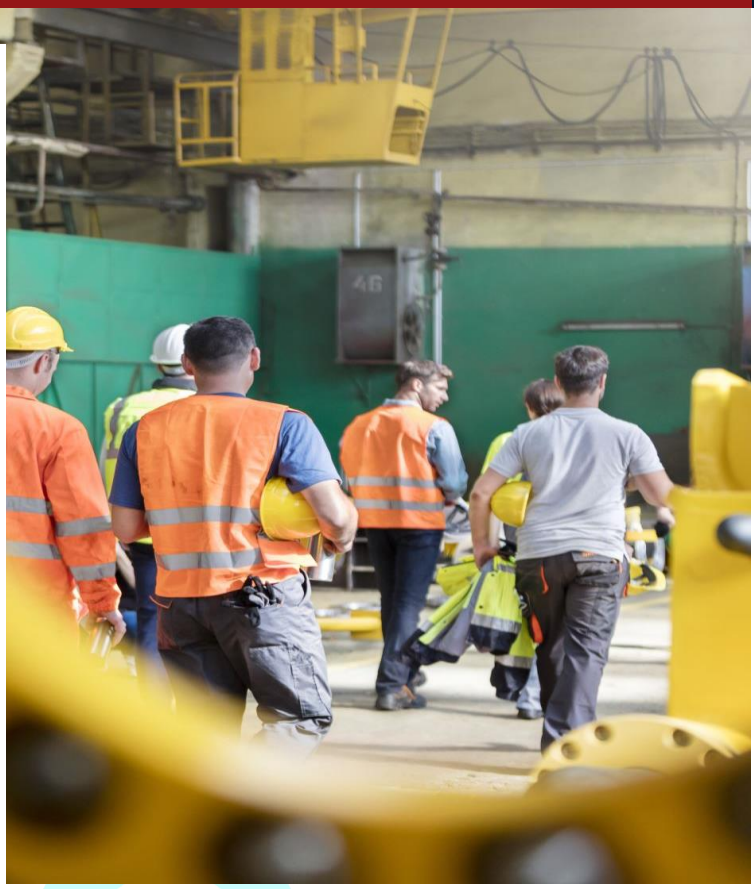
"Just because you're paranoid doesn't mean they aren't out to get you".

In today's hostile cybersphere, a little paranoia may be just what the doctor ordered to keep your confidential business information safe, secure and operationally reliable.

If you need to hire personnel to help implement more robust cybersecurity capabilities for your business, the employer tax incentives outlined in the **Recruiting Roadmap for U.S Employers** on the following pages can provide the additional working capital to do so.

[Click Here to Find Funding for Your Cybersecurity Needs – Up to $33K Per Employee]

Recruiting Roadmap for U.S. Employers



Employer Tax Incentives

2021 & BEYOND

Growth Management Group - GMG

Authored by: John Lynch

"Your Growth is Our Business"

Employee Recruiting Roadmap

Leveraging Employer Tax Incentives

Step 1

Identify & Claim Employee Retention & R&D Tax Credits

Up to $33,000/employee

Step 2

Allocate % of Incentive Payments to Enhance Recruitment Packages

JLynch@GMGSavings.com

Step 3

Pre-screen New Hires for WOTC Tax Credits

Up to $9,600/new hire

Employee Recruiting Roadmap

As a part of the federal pandemic relief package, Congress updated an existing tax credit known as the Employee Retention Credit (ERC) to encourage employers to keep employees on the payroll.

With continued expansions to ERC, nearly every employer qualifies for this tax credit. Employers are encouraged to take advantage of this expansion as each qualified employee can bring up to $33,000 to the employer.

GMG has been helping our clients navigate tax credits for over 15 years. We provide the practical help you need during this time of crisis. A quick look at our online calculator will show you how much your tax credit is.

If you claim the ERC, how will it impact your federal tax return? Per the IRS:

"An employer receiving a tax credit for qualified wages, including allocable qualified health plan expenses, does not include the credit in gross income for federal income tax purposes.

Neither the portion of the credit that reduces the employer's applicable employment taxes, nor the refundable portion of the credit, is included in the employer's gross income."

Who is eligible?

Private employers, including non-profits, that:

- Had operations fully or partially suspended as a result of COVID-19 - OR
- Experienced a significant decline in gross receipts due to the coronavirus.
- Startups also now qualify.
- Employers who received PPP loans are NOW ELIGIBLE FOR ERC CREDITS

Up to $33,000/employee

How much is the tax credit per eligible employee?

- 50% of first $10K in 2020 compensation = $5,000/employee
- 70% of first $10K per quarter in 2021 compensation = $28,000/employee

How is the credit paid?

The credit reduces your employer Social Security tax liability.
If credit is larger than social security tax liability, you will get a direct refund from the IRS for the difference.

The credit is claimed on federal employment tax returns using Form 941, Employer's Quarterly Federal Tax Return.

An amendment can be made to your Form 941 if determined you qualify after you've filed. Eligible employers can file for an advance on the ERC and can claim the credit immediately by reducing payroll taxes to the IRS.

Click here to see an initial estimate of your ERC credits.

Work Opportunity Tax Credits for New Hires

Federal Work Opportunity Tax Credits (WOTC) are general business tax credits for employers that hire job candidates from any of ten categories of underemployed target populations. The credits can offset federal income taxes and can be carried back to the prior year or carried forward 20 years.

Target groups include military veterans, long-term unemployed, SNAP (food stamp) recipient families, empowerment zone residents, summer youth workers and other underemployed target populations (see table below). Tax credits average $2,400 per eligible new hire and, for disabled veterans unemployed for six months or more, are up to $9,600 that is deducted dollar-for-dollar from corporate tax payments.

Recruit More Effectively

Low unemployment and generous unemployment benefits mean record difficulty in recruiting and retaining new hires. One potential use of these tax savings is to redeploy some of it to enhance wages and benefits to better compete for talent in today's highly competitive recruitment arena – making for a "win-win" for employer and employee alike. And when employees *do* move on, you're able to lower your costs of recruiting their replacement by leveraging these tax credit hiring incentives.

Target Populations

Veterans	Long-Term Unemployment Recipients
Long-Term Temporary Assistance for Needy Families Recipients	Short-Term Temporary Assistance for Needy Families Recipients
Supplemental Nutrition Assistance Program (SNAP) Recipients (Food Stamps)	Supplemental Security Income Recipients
Designated Community Residents - 18-39 year olds living in a federally-designated Rural Renewal County or Empowerment Zone	Ex-Felons
Vocational Rehabilitation Referrals	Summer Youth Employees

GMG's paperless process for screening job applicants and optimizing eligibility for WOTC (Work Opportunity Tax Credits) and other hiring tax credits is simple:

- Job candidates answer a few simple questions using our proprietary software.
- You receive instant feedback on potential Local, State, & Federal Hiring Tax Credits.
- Upon hire, we automatically submit the necessary paperwork for approval.
- Once approved, we provide necessary payroll documents to receive the benefit.

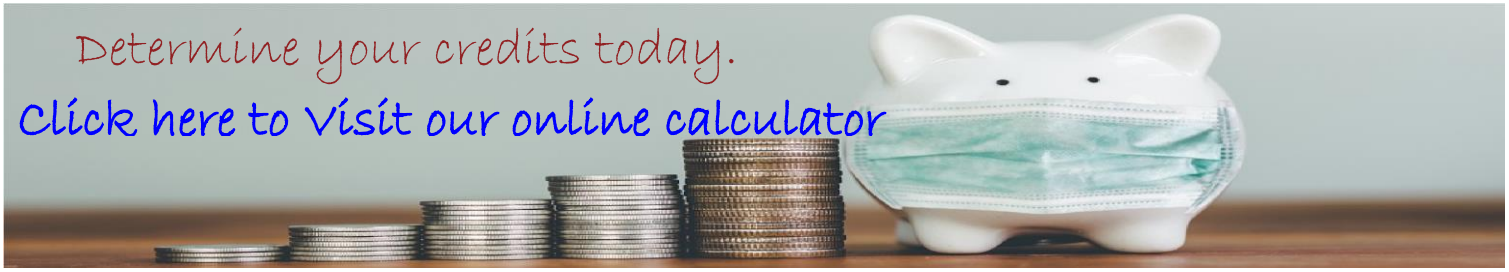
GMG's WOTC service is paperless.

This table reflects GMG's monthly sliding fee schedule for unlimited eligibility searches based on the number of annual new hires.

Max Hires Per Year	Monthly Cost
9	$19
15	$29
25	$49
50	$99
75	$149
100	$199
150	$299
200	$399
200+	Custom

Comparative WOTC Benefits		
	Typical WOTC Provider	GMG
New Hires Annually	100	100
Typical Capture Rate	20%	40%
Qualified Hires	20	40
Average Benefit	$2,400	$2,400
Tax Incentive Savings	$48,000	$96,000
Base Incentive Fee	25%	15%
Net to Employer	$36,000	$81,600
GMG Performance Advantage*		2.26X*

*Before lower processing charges that further improve GMG's performance vs. typical provider ►



Legal Disclaimer

Although the publisher and author have made every effort to ensure that the information in this book was correct at press time and while this publication is designed to provide accurate information in regard to the subject matter covered, the publisher and the author assume no responsibility for errors, inaccuracies, omissions, or any other inconsistencies herein and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

The author is not a cybersecurity professional and the content of this publication is for informational purposes only. This publication is meant as a source of valuable information for the reader; however, it does not constitute legal, financial or cybersecurity advice and is not meant as a substitute for direct expert assistance. If assistance is required, the services of a competent professional should be sought.

The information provided in this book is for informational purposes only and is not intended to be a source of advice or analysis with respect to the material presented. The information and/or documents contained in this book do not constitute legal or cybersecurity advice and should never be used without first consulting with an appropriate professional to determine what may be best for your individual needs.

To the maximum extent permitted by law, the publisher and the author disclaim any and all liability in the event any information, commentary, analysis, opinions, advice and/or recommendations contained in this book prove to be inaccurate, incomplete or unreliable, or result in any data or other losses. No representations or warranties of any kind are made with regard to the content of this publication.

The publisher and the author are providing this book and its contents on an “as is” basis. Your use of the information in this book is at your own risk.