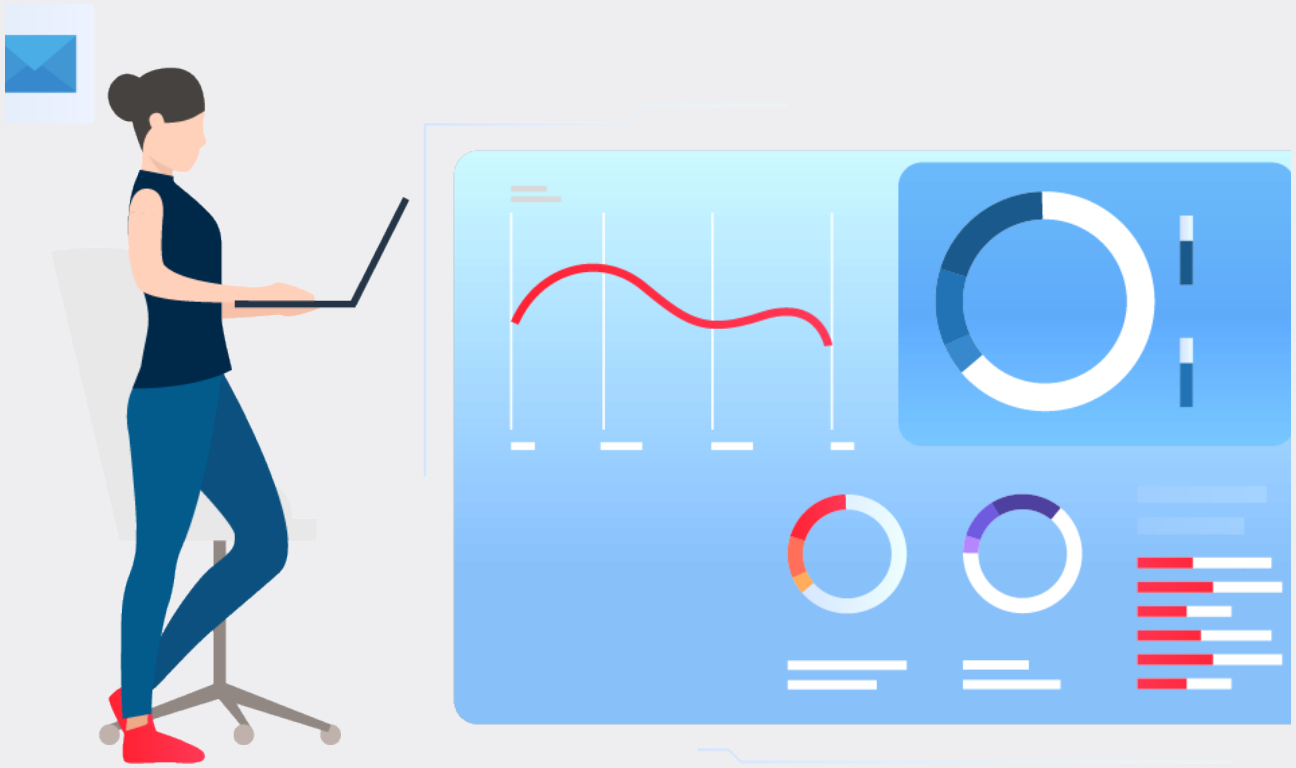
ChatFortress

CYBERSECURITY BUSINESS REPORT



The Most Common Financial Loss Cybersecurity Mistakes Business Owners are Making Today!

This report explains the common mistakes business owners make with their cybersecurity approach and how it's increasing their risk of data breaches, ransomware, and financial loss. Even with in-house or managed IT teams, business owners are continually making these costly mistakes. The following report is based on interviews with executive management, workflow analysis, system review, data analysis, and activities discovered on the corporate system and networks.

WORK PHONE

USA +1 307-999-7755

E-MAIL

Team@ChatFortress.com

URL

www.ChatFortress.com

WHO IS CHATFORTRESS?

ChatFortress

Your Cybersecurity Experts

ChatFortress helps companies reduce their cybersecurity risk by providing companies with the cybercriminal or hackers perspective to their cybersecurity vulnerabilities. This unique human behavioral approach to cybersecurity allows companies to protect their assets from attack and exposure.

ChatFortress is the only company with the next level of security that involves:

- **Selfie-Login: Selfie-Login** - a facial recognition software to visually confirm the actual person and is backed by Home Land Security.
- **Cybersecurity Report Card** - an A-F grading scale report to rate how well your cybersecurity is protecting you personal and professionally.
- **Cybersecurity Conversation Interpretation Technology** – Allows you to understand/measure any potential cyber risk and creates an attack response/recovery plan if an attack is detected within seconds. This historically creates a safe cybersecurity culture by protecting all assets from possible attacks.
- **Managed Solution** – ChatFortress personally manages all cybersecurity threats for you!

EXECUTIVE SUMMARY

__62%__ of businesses experienced phishing and social engineering attacks in 2018

Data compromise happens within every company. ***Our recent study revealed that 90.1% of companies had compromised credentials on the dark web***. Companies don't realize there has been exposure or malicious code installed on machines or BYOD devices. Executives misunderstand cybersecurity priorities due to the outdated methodology sold by many vendors in today's market. The risk of compromise is increasing with social media use.

UNDERSTANDING DATA ASSETS

Using cloud-based solutions does not make you immune from attack!

Many companies fail to understand their data is the most important and valuable asset within their company. **Even if you're using cloud-based solutions, companies need to take control and ownership over their data.** *Assuming your data is safe is a liability waiting to happen.* Many companies don't have a backup of the data within cloud-based systems, let alone known when their vendors have been compromised. Data breaches and ransomware increased in 2019, resulting in companies unknowingly losing their data or being locked out of their software.

Social Engineering is on the rise with increases in Vishing, Smishing and Social Media attacks.

UNDERSTANDING LIKELIHOOD OF ATTACK

By understanding the Likelihood Risk Matrix, companies can better protect themselves from what assets are most likely under attack. **Ransomware attacks increased by 88% in 2019**, with ***9 out of 10 attacks occurring via email.*** *Email* is still one of the most effective channels to compromise a company.

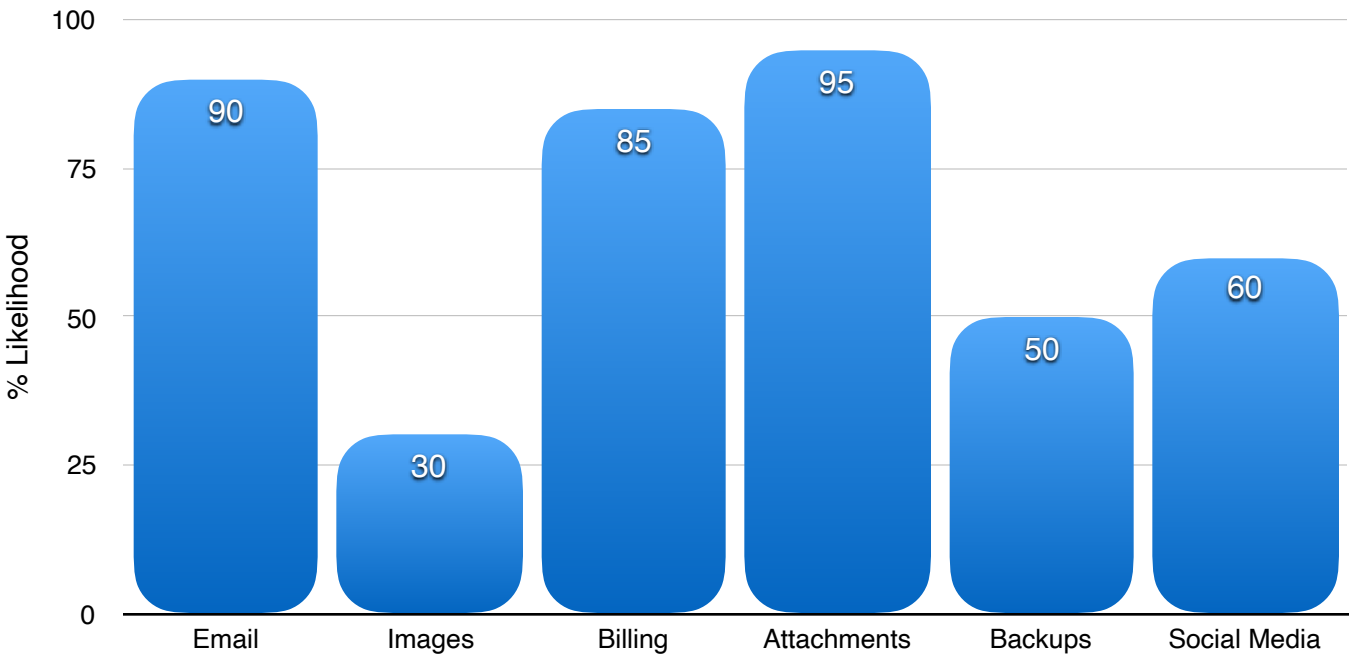
Ransomware attacks will compromise data back-ups to increase the success of a ransomware campaign. ***More often than not, IT managers don't want to admit that data back-up are corrupt or incomplete***. This significantly impacts your downtime after a data breach, and your recovery efforts after a breach is detected.

Our likelihood matrix shows you the top six types of attacks and what will be compromised within those attacks to help you eliminate trouble before it happens.

It's not if you will be attacked...
it's what happens when you are attacked?

THE AVERAGE DATA BREACH COSTS $200,000 PLUS RECOVERY DAMAGES

HOW CYBERCRIMINALS WILL ATTACK YOUR COMPANY



COMPROMISED DATA

Companies set up password change protocols. But *forget to implement protocols* to change their social media passwords or other online accounts. Your cybersecurity culture should empower all users to change all their passwords regularly. ***36% of people still use the same password for more than one account***. Because of this hackers are increasingly using social engineering or open-source intelligence strategies to compromise your accounts and steal your data. The telephone is the new threat vector for caller ID spoofing or compromise.

71% of breaches were financially motivated *and 25% were motivated by espionage.*

Completing regular audits of every service you and each employee uses online or offline should be part of your quarterly security audit. It's amazing the number of accounts created by employees without thought of data compromise, or audit trails. For example an increasing number of employees leave companies to attacks due to forgotten social media accounts.

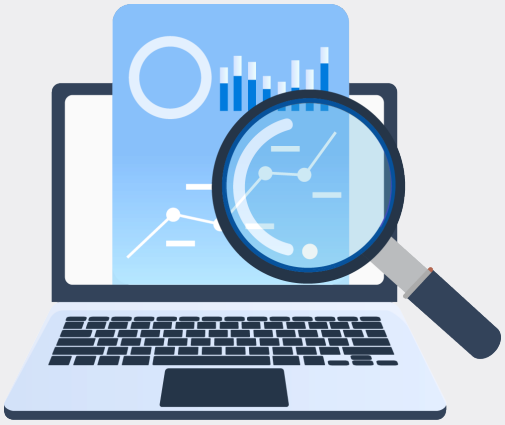
52% of breaches featured hacking, 28% involved malware and ***32–33% included phishing or social engineering****.*

2019 resulted in billions of personalized data records being stolen. ChatFortress believes that spoofing and impersonation frauds will continue to increase and leverage this personalized attack data. Unfortunately in these current times cybercriminals know who your friends and family are, they will use this information to compromise everyone and everything to their advantage. ***Hackers don't care about you or the harm they cause you. Hackers care about getting paid for their exploits.***

UNDERSTANDING MAXIMUM TOLERABLE DOWNTIME

MAXIMUM TOLERABLE DOWNTIME CALCULATION

Do you know your *Maximum Tolerable Downtime? (MTD)*
Do you know your *Restore Point Objective (RPO)? This is h*ow much data may be ***lost*** during a disaster? How long will it take you to recover this data and what happens to the rest of your business during this time?



MAXIMUM TOLERABLE DOWNTIME

This is the time you can afford to be without access to any one of your systems within your business. It's knowing that when you experience a breach, you have allocated a budget and timeline for a response. Many companies don't factor in the response and recovery cycles. Dealing with the attack is different from recovering from the attack.

After a ransomware attack, can your company afford to be down for 14 days or more during the recovery process? *This is not including the initial response times, but the recovery time to regain access to systems and data. Could you afford this downtime?*

Service	MTD	RPO
Email Access		
Accounts & Billing		
CRM or ERP Service		
Social Media Accounts		
Server Access		

How long can your business afford to not have access to your data, or your computers?

URGENT ISSUES

HACKED CREDENTIAL DARK WEB MONITORING

36% of people use the same password for more than one service. *Believe it or not,* hackers can likely already login to your accounts using your username and passwords they find on the dark web. Companies are not using dark web monitoring services to create feedback loops for high-risk accounts, or any account associated with your domain. Receiving alerts about third party compromise allows you to protect your people and your network. Even if the employee is no longer with the company, have you validated their access has been removed from all services? *It's easy to remove the email account but leave the social media accounts that the employee used.*

RANSOMWARE SIMULATION

Ransomware attacks increased by 88% in 2019. Your network may not be as secure as you think. Companies are failing to effectively test their networks against ransomware attacks. ***Most companies fail a ransomware simulation***, with a high percentage of companies losing access to their backup systems.

If you get hacked today, how long will it take you to discover the compromise?

Most companies range from 4 months to 14 months to discover a data breach.

Depending on how reactive you are to a hack determines your survivability.

MONITORING NETWORK TRAFFIC

Cybercriminals will patiently wait until your system is most vulnerable to strike, *such as after regular working hours or when your core staff is on vacation*. If there is a time when your network is weak, you can be sure some enterprising hacker will choose that time to launch their attack. **One of the critical elements that determine how devastating a cyberattack will be on your company is how fast is your response to the attack**. You need to understand that If there is an attempt to breach your system, every minute that you are not aware of the breach is a minute you are not stopping the attack. **It's also a minute where you could be losing valuable megabytes of data each minute it's unnoticed.** ***How do you detect attacks and respond now?***

EMAIL PHISHING DETECTION & SIMULATION

Email is the unlocked front door of many cyber-attacks. Cybercriminals have been layering malicious emails with phone calls and text messages as part of their attack strategy. Real-time detection and mitigation of bad emails are required to protect all email users. Many email services don't provide bad email detection or removal, leaving companies exposed to attack. ***0***. Email phishing simulation should occur monthly as part of your cybersecurity awareness program with a real-world testing matrix. **We have seen companies receive upwards of 1,600 bad attack emails per day!**

THREAT ANALYSIS

The biggest threat is thinking you're immune or safe from attack!

RANSOMWARE

Ransomware trends are high – Users are inadequately trained in detection and response strategies. Knowing the response procedures for when a ransomware attack occurs is essential training for all team members. ***Mobile device attacks are increasing***, therefore, taking steps to protect every device even BYOD mobile devices is important.

DATA THEFT

Malware activity found on 90% of networks. Current Anti-Virus products are not robust enough to detect and stop current web-threat technology. This requires real-time monitoring with a response plan. The problem with this situation, is that many companies are installing "protective"software, but no one is monitoring this software! Data is your most valuable asset, and this is like leaving the keys in your car while leaving a bag of cash on the front seat. Hoping that no one steals your money or car is not an effective strategy. ***Cybercriminals are equal opportunity offenders if the opportunity exists; it's only a matter of time before you experience a fraud.***

EMAIL SPOOFING AND IMPERSONATION

Email spoofing and impersonation attempts have been successful for invoice fraud and wire transfers. Email is not a secure channel for processing payments or validating sensitive information.

TELEPHONE PHISHING AND SOCIAL ENGINEERING

Attackers are increasingly using the telephone as part of their scams. Setting up procedures for a call back or validation of caller identity along with validation of information received will protect callers from these types of scams. Using PIN codes or two-factor authentication can protect sensitive data.

*Hackers attack every **39 seconds**, on average 2,244 times a day*

43% of cyber attacks target small business!

95% of data breaches occur due to human error. *With 77% of companies not having a response plan.*

CYBERSECURITY PROTOCOL

Companies ***spend and waste a lot of money*** on prevention strategies. The most critical element of any cybersecurity strategy is the detection and response stages of your protocol. Cybercriminals will breach your network, and the key question is, how long will it take you to discover the breach, and what do you do next?

Many companies have little or no detection and response plans. Even Target.com was aware of its data breach for four months before they took action. Waiting to take action significantly increased the recovery cost. Learn more about common cybersecurity mistakes at www.ChatFortress.com/CommonCybersecurityMistakes

PROTECTION IS NOT ENOUGH

Protection is not enough. This is like having a fire alarm in your house without anyone calling the fire department.

Companies have been sold by vendors that protection alone is enough. But it's really the second step of a 5 step approach to cybersecurity.

Detecting smoke and then calling the fire department is what will protect your home from burning down. We often see companies that have ineffective detection software and it's that's not configured correctly or reporting to anyone. Therefore the response plan is never activated.

Do you have a detection strategy and response strategy in place that you have validated?

NEXT STEPS?

Contact ChatFortress for a **Free cybersecurity assessment.** Allow our team to review your system and give you the hackers' perspective on your cybersecurity risk.

ChatFortress will work with your existing IT team to provide them with a cybersecurity blueprint on exactly how you can reduce your cybersecurity risk.

WWW.CHATFORTRESS.COM/DEMO

CALL USA +1 307-999-7755

WHAT'S INCLUDED WITH YOUR FREE CYBERSECURITY ASSESSMENT?

- Our risk and liability assessment covers all the potential holes in your network so we can plug them up before a malicious actor finds them. Whether your problem is inadequate data protection, failure to attend to third-party risks, a lack of awareness of potential threats or other vulnerability issues, we'll find them and let you know about them right away – so you can clear them up fast.
- ChatFortress will expose any of your user credentials that are exposed on the dark web as part of our Hacked Dark Web Scan.
- ChatFortress will review your current email phishing and impersonation detection and mitigation systems and provide recommendations on the action you can take to protect all users on your network.

SCHEDULE YOUR CYBERSECURITY ASSESSMENT TODAY